Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

Dados pessoais para o desenvolvimento econômico, tecnológico a inovação

GTT 5

2025

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

GT5 – SUBSÍDIOS PARA A PNPD

DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

RELATÓRIO FINAL E PARECER CONCLUSIVO

04/02/2025

Rony Vainzof (Coordenação)

Alexandre Zago Boava

Cassio Augusto Muniz Borges

Débora Sirotheau Siqueira Rodrigues

Fábio Veras de Souza

Isabella Henriques (participante)

Myreilla Aloia Triumpho Pereira da Cruz

Vitor Morais de Andrade

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

SUMÁRIO

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

1. CONTEXTUALIZAÇÃO E OBJETIVOS DO GT5

Ao logo das últimas décadas dados pessoais se consolidaram como insumo fundamental para a execução de políticas públicas eficientes e o impulsionamento do mercado. Seu valor e influência decisiva permeiam desde a prevenção a fraudes, proteção ao crédito, medicina preditiva, cidades inteligentes e gestão pública até o marketing direcionado, comércio digital e o desenvolvimento da inteligência artificial. Com isso, dados pessoais tornam-se não apenas alicerces para transações econômicas e políticas de Estado, mas também vetores de transformação para toda a sociedade.

Não é por acaso que a Lei Geral de Proteção de Dados (LGPD) traz como fundamento a proteção de dados pessoais para o desenvolvimento econômico, tecnológico e a inovação, conforme previsto em seu art. 2º, inc. V, refletindo a proteção de direitos fundamentais como forma de estimular a inovação responsável e a competividade sustentável.

Se dados pessoais são catalisadores da economia digital, a LGPD, a sua interpretação, bem como a futura Política Nacional de Proteção de Dados (PNPD), são instrumentos necessários e relevantes para que o desenvolvimento econômico, tecnológico e a inovação possa caminhar ao lado da privacidade, proteção de dados pessoais e da preservação de outros direitos fundamentais.

Assim, conforme Portaria CNPD nº05/2024[1], o GT 5 buscou explorar, entender e, ao final, prover subsídios para a PNPD acerca da proteção de dados pessoais como forma de inovação responsável e de como a LGPD legitima o uso lícito, seguro e ético dos dados pessoais para o desenvolvimento econômico, tecnológico e a inovação.

2. MEMBROS DO GT5

Membros	Setor
Rony Vainzof (coordenador)	Empresarial
Alexandre Zago Boava	Laboral
Myreilla Aloia Triumpho Pereira da Cruz	Produtivo

[1] Portaria CNPD nº 05, de 4 de outubro de 2024 Institui o Grupo de Trabalho, dedicado a fornecer subsídios, na temática de dados pessoais para o desenvolvimento econômico, tecnológico e a inovação, para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade, no âmbito do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade.

Vitor Morais de Andrade	Empresarial
Fábio Veras de Souza	Senado Federal
Débora Sirotheau Siqueira Rodrigues	Laboral
Cassio Augusto Muniz Borges	Produtivo
Isabella Henriques (participante)	Sociedade Civil

3. ENTREVISTAS

As entrevistas buscaram colher subsídios para um diagnóstico melhor do problema, de acordo com um roteiro previamente estabelecido.

Entrevistada: Miriam Wimmer

Diretora da ANPD. Doutora em Políticas de Comunicação e Cultura pela Faculdade de Comunicação da UnB, Mestre em Direito Público e graduada em Direito pela UERJ. Certificada como especialista em proteção de dados pessoais (Europa) pela *International Association of Privacy Professionals* (CIPP/E). Ocupou diferentes cargos de direção no Ministério das Comunicações - MC e no Ministério de Ciência, Tecnologia, Inovações e Comunicações - MCTIC, onde coordenou a elaboração da Estratégia Brasileira para a Transformação Digital. Desenvolve atividades profissionais e acadêmicas em temas ligados à Internet, às telecomunicações, às políticas digitais e à proteção de dados pessoais.
Data: 13/11/24
Ata da entrevista: Anexo I

Entrevistado: Lucas Borges de Carvalho

Gerente de Projetos da ANPD. Possui graduação em Direito pela Universidade Federal da Bahia - UFBA (2003), mestrado em Direito pela Universidade Federal de Santa Catarina - UFSC (2006) e doutorado em Direito pela Universidade de Brasília - UnB (2015). Procurador Federal da Advocacia-Geral da União desde 2007. Entre outros órgãos públicos, atuou na Consultoria Jurídica do Ministério das Comunicações, na Consultoria Jurídica do Ministério da Cultura e na Procuradoria Federal Especializada da Anatel. Tem experiência docente, tendo atuado como professor substituto da UFSC e da UnB, entre outras instituições.
Data: 13/11/24
Ata da entrevista: Anexo I

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

Entrevistado: Renan Kalil

Ministério Público do Trabalho. Professor de Direito no Insper. Doutor e Mestre em Direito pela Universidade de São Paulo. (2019 e 2012). Especialista em Direito Aplicado ao Ministério Público do Trabalho pela Escola Superior do Ministério Público da União (ESMPU). Graduado em Direito com especialização em Direito do Trabalho e da Seguridade Social pela Faculdade de Direito da Universidade de São Paulo (FD-USP).
Data: 13/11/24
Ata da entrevista: Anexo I

Entrevistado: Fabrício da Mota Alves

Advogado especialista em Direito Digital. Tem vasta experiência na área, tendo participado ativamente no processo legislativo que levou à edição da Lei Geral de Proteção de Dados Pessoais brasileira. Foi assessor legislativo sênior do Senado Federal e participou da Comissão de Juristas que elaborou o projeto de lei de regulação da Inteligência Artificial no Brasil. Coordenador jurídico da Frente Parlamentar de Proteção de Dados da Câmara dos Deputados. Representante do Senado Federal no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (1ª composição), órgão que compõe a Autoridade Nacional de Proteção de Dados. Professor de Proteção de Dados em São Paulo (Insper, LEC, Escola Paulista de Direito e Opice Blum *Academy*), Distrito Federal (IDP e ATAME), Paraná (PUC), Rio de Janeiro (FGV) e Recife.
Data: 03/12/24
Ata da entrevista: Anexo II

Entrevistado: Fabrício Guimaraes Madruga Lopes

Coordenador-Geral de Fiscalização da ANPD. Especialização em Regulação de Serviços Públicos de Telecomunicações – Pós-graduação, Universidade de Brasília, concluído em 2009. Direito – Graduação, Universidade de Brasília, concluído em 2002. *Data Protection Academy's Course – Maastrich University, Faculty of Law* (2021).
Data: 12/12/24
Ata da entrevista: Anexo III

Entrevistada: Fabiana Silva Pinto Faraco Cebrian

Coordenadora-Geral de Tecnologia e Pesquisa da ANPD. Engenheira. Mestre em Ciências pelo Instituto Militar de Engenharia IME, área de concentração Tecnologia da Informação Geográfica. Advogada. Mestre em Direito

Socioambiental e Sustentabilidade pela Pontifícia Universidade Católica do Paraná PUCPR. Professora de cursos de curta duração e de pós-graduação nos cursos de Direito Digital, *Big Data e Marketing Intelligence*, Arquitetura de Software, Ciência de Dados e *Cybersecurity,* Direito 4.0, *Legal Operations*, Direito Societário e Contratos Empresariais. Pesquisadora Sênior do GEDAI – Grupo de Estudos de Direito Autoral e Industrial da Universidade Federal do Paraná.
Data: 12/12/24
Ata da entrevista: Anexo III

Entrevistado: Rodrigo Santana dos Santos

Coordenador-Geral de Normatização da ANPD. Mestrado em Engenharia Elétrica – Telecomunicações.
Data: 12/12/24
Ata da entrevista: Anexo IV

Entrevistado: Eduardo Gomes Salgado

Coordenador-Geral de Relações Institucionais e Internacionais da ANPD. Pós-Doutor em Engenharia de Produção *University of Glasgow*– Adam Smith *Business School* – Escócia (2014 a 2015). Doutor em Engenharia Mecânica Universidade Estadual Paulista Júlio de Mesquita Filho – UNESP (2008 – 2011). Mestre em Engenharia de Produção Universidade Federal de Itajubá - UNIFEI (2006 – 2008). Graduação em Engenharia de Produção Universidade Federal de Itajubá - UNIFEI (2001 – 2005).
Data: 12/12/24
Ata da entrevista: Anexo IV

Entrevistado: Ronaldo Lemos

Mestre em Direito pela Universidade de Harvard e doutor pela USP. Professor da Universidade de Columbia, colunista do jornal Folha de S. Paulo, da revista Trip e da Globonews. Além disso, é um dos criadores do Marco Civil da Internet. Reconhecido internacionalmente por ser especialista em temas como tecnologia, dados, mídia e propriedade intelectual.
Data: 13/12/24
Ata da entrevista: Anexo V

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

4. CONTRIBUIÇÕES DE ENTIDADES

Visando colaborar com o desenvolvimento dos trabalhos do GT 5, entidades de diversos setores e da sociedade civil foram oficiadas solicitando contribuições, conforme o objeto pretendido no trabalho. As respostas encontram-se em anexo, em ordem alfabética:

1) Associação Brasileira de Empresas de *Software* (ABES) - Anexo VI;
2) Associação Brasileira de Mobilidade e Tecnologia (AMOBITEC) – Anexo VII;
3) Associação das Empresas de Tecnologia da Informação e Comunicação e de Tecnologias Digitais (Brasscom) – Anexo VIII;
4) Associação Nacional dos *Bureaus* de Crédito (ANBC) – Anexo IX;
5) Conexis Brasil Digital - Anexo X;
6) Federação Brasileira de Bancos (FEBRABAN) – Anexo XI;
7) IAB Brasil – Associação de Mídia Interativa - Anexo XII;
8) Instituto Nacional de Proteção de Dados (INPD) – Anexo XIII;
9) Ministério Público do Trabalho (MPT) – Anexo XIV;
10) Movimento Brasil Competitivo (MBC) – Anexo XV;
11) Universidade Federal Rural de Pernambuco (URFPE) – Anexo XVI;
12) Instituto Alana – Anexo XVII.

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

5. ESTUDOS DE CASO

Foram desenvolvidos Estudos de Caso pelos Conselheiros do GT, apresentando informações e análises necessárias para subsidiar o Parecer Conclusivo, contendo os seguintes itens e objetivos:

Práticas Nacionais e Internacionais: casos práticos e dados estatísticos que demonstram a importância do uso e da proteção de dados pessoais para o desenvolvimento econômico, tecnológico e a inovação responsável.

Conformidade legal e uso ético no Brasil e em outras Jurisdições: como a LGPD e outras normas aplicáveis, nacionais e internacionais, servem como bússola para que os dados pessoais possam ser utilizados para o desenvolvimento econômico, tecnológico e a inovação, de forma ética, segura e responsável.

Meios para aumentar a proteção de dados e segurança jurídica: práticas como dados abertos; infraestruturas digitais; códigos de boas práticas para compartilhamento; acordos com a administração pública; *Privacy Enhancing Technologies* – PETs; interlocução com os demais órgãos reguladores setoriais; e harmonização com as demais Políticas e Estratégias nacionais poderiam destravar o uso de dados pessoais, respeitando os direitos e garantias fundamentais, a LGPD e demais normas aplicáveis.

- Inteligência Artificial – Anexo XVIII
  Conselheiro responsável: Rony Vainzof.

- Prevenção a Fraudes e Autenticação/Identificação Digital – Anexo XIX
  Conselheiras responsáveis: Myreilla Cruz e Débora Sirotheau.
  Especialista convidada: Martha Leal.

- Proteção ao crédito –Anexo XX
  Conselheiro responsável: Rony Vainzof.

- Contexto Laboral – Anexo XXI
  Conselheira responsável: Débora Sirotheau.
  Especialistas convidados: Carlos Fernandes Coninck Júnior; Caroline de Melo Lima Goularte; e Selma Carloto.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

- Empreendedorismo e empreendedorismo social – Anexo XXII
  Conselheiro responsável: Alexandre Boava.

- Educação e Inclusão - Anexo XXIII
  Conselheira responsável: Isabella Henriques.

- Cidades Inteligentes - Anexo XXIV
  Conselheiro responsável: Rony Vainzof.

- Crianças e Adolescentes - Anexo XXV
  Conselheira responsável: Isabella Henriques.

- Acesso ao Poder Público – Anexo XXVI
  Conselheiro responsável: Alexandre Boava.

- Eficiência Energética e Sustentabilidade – Anexo XXVII
  Conselheiro responsável: Cassio Borges.
  Especialista convidado: Wagner Ferreira.

- Marketing e Publicidade – Anexo XXVIII
  Conselheiro responsável: Vitor Moraes de Andrade.

- Saúde – Anexo XXIX
  Conselheiro responsável: Rony Vainzof.

6. REUNIÕES

Ao longo dos 4 (quatro) meses de trabalho, desde a instituição do GT5, em 04 de outubro de 2024, foram realizadas diversas reuniões ordinárias e extraordinárias. As atas delas foram encaminhadas à Secretaria-Geral para fins de transparência e arquivo.

7. PARECER CONCLUSIVO

Diante de todo o trabalho exposto e consignado neste Relatório Final e respectivos anexos, o GT 5 do CNPD fornece os seguintes subsídios, na temática de dados pessoais para o desenvolvimento econômico, tecnológico e a inovação, para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade (PNPD):

1. O desenvolvimento econômico, tecnológico e a inovação é também pautado no tratamento e circulação dos dados pessoais, conforme demonstrado nos Estudos de Caso e constante nas mais variadas estratégias, planos e políticas de Estado. Porém, o tratamento de dados pessoais não pode ser feito sem observar a legislação, especialmente a Lei Geral de Proteção de Dados Pessoais (LGPD), de forma a garantir os direitos dos titulares. Assim, é preciso ampliar a percepção da proteção de dados pessoais como condição e indutor para o desenvolvimento econômico, tecnológico e a inovação, nos termos do art. 2º, inc. V, da LGPD;

2. A Política Nacional de Proteção de Dados deve refletir o equilíbrio dos dois principais objetivos da LGPD: (i) proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural; e (ii) permitir geração de valor e ser base do desenvolvimento econômico a partir do tratamento e circulação dos dados pessoais, desde que sejam realizados de forma lícita;

3. A LGPD é instrumento para a inovação e não deve ser vista ou interpretada como entrave para o desenvolvimento econômico e tecnológico. Associado a isto os dados devem ser tratados de forma a beneficiar todos os titulares de dados;

4. Estimular a prática do *Privacy by Design* nos setores público e privado, pois, ao integrar a proteção de dados pessoais desde a concepção de produtos, serviços e processos, a abordagem equilibra inovação, desenvolvimento econômico e proteção de dados e privacidade, contribuindo com:

    a) O fomento à confiança do indivíduo: os agentes de tratamento ganham credibilidade e aumentam a fidelização, o que impulsiona o consumo e fortalece a reputação no mercado e dos serviços públicos;
    b) Redução de riscos e custos relacionados a multas, indenizações e incidentes;
    c) Impulso à inovação e à eficiência: quando a privacidade é implementada desde o início, além de os agentes de tratamento terem visibilidade total acerca de novos produtos e serviços que envolvam dados pessoais, não será necessário fazer mudanças estruturais ou funcionais neles, posteriormente, para atender às regulamentações, como a LGPD. Essas alterações posteriores podem ser custosas, tanto financeiramente quanto em termos de tempo. O *PbD* também torna processos mais ágeis, transparentes e explicáveis e ao evitar a coleta excessiva de dados, os

agentes de tratamento economizam custos de armazenamento, processamento e descarte. Por fim, estimula a criação de soluções tecnológicas avançadas, como anonimização, criptografia e design ético, que atendem às demandas do mercado e às exigências regulatórias; e

d) Competitividade global: empresas se alinham a padrões internacionais, ganhando vantagem competitiva em mercados globais.

5. Dentro da prática do *Privacy by Design*, estimular*:*
   a) A incorporação a priori dos princípios e garantias da LGPD desde as etapas iniciais do desenvolvimento do produto digital, passando pelo seu desenho, implementação e testes;
   b) Uma abordagem multinível para verificar a conformidade com os princípios da LGPD em diferentes estágios do desenvolvimento, de acordo com o nível de risco das atividades de tratamento;
   c) Funcionalidades que permitam aos usuários exercerem seus direitos, criando interfaces e fluxos que promovam a transparência sobre o uso e tratamento de dados pessoais;
   d) O desenvolvimento de glossário centralizado ou a ser distribuído nas aplicações que fortaleça a compreensão da política de privacidade e proteção de dados adaptado ao contexto de sistemas de software, e desenvolver checklists e quadros de apoio para cada princípio da LGPD;
   e) Medidas técnicas e administrativas para garantir a segurança e prevenção de incidentes, adotando práticas de minimização de dados, coletando apenas o necessário para as finalidades específicas e legítimas; e
   f) Tecnologias de Anonimização e Pseudonimização devem ser estimuladas, quando possível, reduzindo os riscos associados ao tratamento de dados pessoais, especialmente para o treinamento de IA.

6. Estimular práticas de proteção de dados por meio de incentivos regulatórios e econômicos, beneficiando tanto o setor público quanto o privado, como nos seguintes exemplos:
   a) Linhas de crédito específicas, oferecidas por bancos públicos ou privados, para pequenas e médias empresas investirem em adequação à proteção de dados;
   b) Subsídios ou descontos tributários vinculados à certificação em proteção de dados;
   c) Acesso a linhas de crédito ou subsídios para projetos de inovação relacionados à proteção de dados;
   d) Prioridade em licitações e contratos públicos; e
   e) Divulgar ranking público destacando empresas e organizações com as melhores práticas de governança em proteção de dados.

O Conselheiro Alexandre Boava apresentou parecer divergente apenas em relação aos itens 6.b, 6.d e 6.e, conforme os seguintes fundamentos:

Subsídios ou descontos tributários vinculados à certificação em proteção de dados: essa prática pode se tornar mais um mecanismo de incentivo fiscal, sobretudo, para grandes empresas que já se beneficiam de outras políticas de incentivo. A proteção de dados é um direito fundamental e não deve ser estimulada via contrapartidas econômicas, outros mecanismos de apoio e responsabilização devem ser estimulados.
Prioridade em licitações e contratos públicos: essa prática pode criar um acúmulo de contratos para empresas que já tem em seus processos práticas de proteção de dados por conta dos riscos associados a operação em detrimento de outras que, por serem menores ou não estarem associadas a um alto risco, não tenham práticas sofisticadas em nenhum grau do tratamento de dados pessoais.
Divulgar anualmente um ranking público destacando empresas e organizações com as melhores práticas de governança em proteção de dados: a prática de rankings é muito questionável por acabar favorecendo empresas que influenciam o executor do ranking. Salvo se esse ranking for feito pelo governo (ANPD) com transparência para a população.

7. Estabelecer diretrizes para que empresas entendam a privacidade como diferencial competitivo, estimulando soluções tecnológicas éticas e centradas no usuário;

8. Implementar o conceito de *Fair Design Patterns*, que promove a experiência mais ética e respeitosa, priorizando a autonomia do usuário, a transparência na coleta e no uso de dados, e a facilidade de acesso a configurações de privacidade. É a antítese dos padrões obscuros de design;

9. Incentivar o uso de técnicas de *Legal Design* e *Visual Law* para estimular o desenvolvimento de políticas de privacidade claras, acessíveis e compreensíveis aos titulares dos dados. A linguagem deve ser simples, objetiva e livre de jargões técnicos ou termos jurídicos complexos, assegurando uma comunicação eficaz. Além disso, o design da informação deve priorizar a organização visual e hierarquia clara, utilizando recursos gráficos e estruturais que facilitem a navegação, a assimilação e a interação, promovendo uma experiência inclusiva e transparente;

10. Ressaltar a importância de o controlador fornecer, sempre que solicitado, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial, bem como acerca do direito que os titulares têm de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade;

11. Promover a transparência e explicabilidade sobre o uso de dados pessoais em sistemas de IA, fornecendo informações claras aos titulares sobre como seus dados são utilizados;

12. Promover padrões para governança e interoperabilidade de dados, permitindo o uso compartilhado em setores estratégicos sem comprometer a segurança e a privacidade;

13. Promover espaços de dados pessoais como ecossistemas integrados, regidos por políticas claras, para fomentar a economia de dados. A Administração Pública deve ampliar a política de dados abertos em conjunto com a inciativa privada para dados que são produzidos em espaços públicos, compartilhando proativamente informações relevantes, acessíveis e reutilizáveis com todas as partes interessadas. Isso facilita inovações e colaborações entre governo, setor privado e sociedade, além de permitir transações complexas com regras claras sobre o uso de dados. Recomenda-se a criação de um Comitê Multissetorial, envolvendo governo, sociedade civil, academia, setor produtivo e representação de trabalhadores, para orientar políticas públicas de dados abertos. Os dados pessoais compartilhados nos espaços de dados devem ser tratados em consonância com a LGPD;

14. A ANPD deve estar ao lado dos demais Órgãos Setoriais, Legislativo, Executivo e Judiciário, por meio de cooperação interinstitucional, para que políticas de Estado já nasçam, desde a sua concepção, seguindo o princípio do *Privacy by Design*;

15. A ANPD, de acordo com as suas competências, deve desempenhar o papel na conexão e equilíbrio entre Direito e inovação, pois não se antagonizam. Pelo contrário, devem caminhar juntos;

16. Estimular o fortalecimento e maior autonomia institucional da ANPD,[2] como forma de proteção a direitos e gerar maior segurança jurídica;

17. Fortalecer a cooperação com o setor privado e a sociedade civil, por meio de instrumentos como os Acordos de Cooperação Técnica e o fórum de comunicação permanente previsto na LGPD;

18. Reconhecer a importância da Análise de Impacto Regulatório como ferramenta para avaliar as intervenções regulatórias e minimizar os impactos negativos sobre os agentes econômicos e a sociedade;

19. Aprimoramento do processo de monitoramento regulatório (Avaliação de Resultado Regulatório e Monitoramento do Ambiente Regulado);

[2] Por exemplo- Ações Educativas: criação de uma área dedicada a ações educativas para promover a cultura de proteção de dados no país. Comunicação: criação de uma assessoria de comunicação para melhorar a comunicação da ANPD com a sociedade. Assessoria Parlamentar: criação de uma assessoria parlamentar independente para fortalecer a interlocução da ANPD com o Legislativo. Autonomia: garantir maior autonomia à ANPD, permitindo que ela atue de forma independente.

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

20. Apoiar iniciativas acadêmicas, empresariais e populares em Pesquisa & Desenvolvimento relacionadas à proteção de dados e privacidade, fortalecendo a base tecnológica do país;

21. Criar zonas regulatórias experimentais (*sandboxes* regulatórios) para empresas de qualquer natureza testarem soluções tecnológicas, de forma controlada e monitorada pela ANPD;

22. Decisões de adequação e o reconhecimento de cláusulas-contratuais equivalentes orientadas pela ANPD são fundamentais para tornar mais seguro ao titular de dados o fluxo internacional de seus dados pessoais;

23. Os princípios da finalidade, adequação e necessidade, previstos na LGPD, devem ser interpretados de maneira que permitam usos futuros compatíveis com o propósito original, garantindo segurança jurídica e inovação, especialmente no uso de dados para treinamento da Inteligência Artificial[3];

24. Não há hierarquia entre as bases legais autorizativas para o tratamento de dados pessoais previstas na LGPD. Em termos do desenvolvimento econômico, tecnológico e a inovação, uma das principais discussões envolve a utilização adequada e lícita, principalmente, das bases legais do consentimento e do legítimo interesse. O fenômeno da fadiga do consentimento[4] precisa ser endereçado com transparência ativa ("consentimento informado"), avaliação dos mais variados níveis de hipossuficiência ("livre") e novas formas, como o *legal design* e *visual law*, para a manifestação do titular ("inequívoco"), como previsto na própria LGPD. Já o interesse legítimo permite que as organizações tratem dados quando têm um interesse genuíno e válido, desde que este não prejudique os direitos e liberdades dos indivíduos. Esta base legal deve ser acompanhada por fortes obrigações de responsabilização e avaliação de risco, garantindo a proteção dos indivíduos. Ainda, ela é contextual e requer uma avaliação caso a caso, além de o indivíduo ter o direito de se opor ao tratamento de seus dados sob o interesse legítimo, em caso de descumprimento da legislação;

---

[3] Conforme Estudo de Caso da IA. CIPL. The Limitations of Consent as a Legal Basis for Data Processing in the Digital Society. 2024. Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_bkl_limitations_of_consent_legal_basis_data_processing_dec24.pdf

[4] A quantidade e complexidade da informação necessária para os indivíduos darem consentimento informado são tão grandes que se torna quase impossível para eles assimilarem tudo antes de tomar uma decisão, o que resulta no fenômeno da "fadiga de consentimento". Vide Estudo de Caso da IA. CIPL. The Limitations of Consent as a Legal Basis for Data Processing in the Digital Society. 2024. Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_bkl_limitations_of_consent_legal_basis_data_processing_dec24.pdf

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

25. As ponderações acerca da base legal adequada devem ser ainda mais criteriosas em se tratando do tratamento de dados de crianças e adolescentes, especialmente para atender o consentimento qualificado, conforme artigo 14 da LGPD e nos termos da Res. 245/24, do CONANDA;

26. Prevenção ao cibercrime e a fraudes envolvendo dados pessoais:

a) Fomentar frentes que objetivem a redução de ilícitos relacionados a dados pessoais, em conexão e cooperação com políticas de segurança pública;
b) Promover campanhas educativas para a população, destacando os riscos de fraudes cibernéticas e como proteger seus dados pessoais em transações online;
c) Criar canais acessíveis para que cidadãos possam reportar fraudes e obter orientação sobre como proteger seus dados em caso de incidentes, permitindo a coleta e análise de dados de incidentes e auxiliando na identificação de padrões e ameaças;
d) Estabelecer parcerias entre instituições públicas e privadas para a troca de informações e o desenvolvimento de estratégias conjuntas de prevenção a fraudes, sempre observando os limites legais de compartilhamento de dados;
e) Implementação de ferramentas para monitorar e identificar atividades suspeitas em tempo real;
f) Implementação de soluções e sistemas para garantir maior segurança nos processos de autenticação e identificação de identidade;
g) Implementação de protocolos que propiciem rastreamento e recuperação rápida de perdas;
h) Medidas de cibersegurança integrada entre todas as áreas envolvidas no processo;
i) Incentivo à inovação e pesquisa fomentando o desenvolvimento de soluções para prevenção à fraude baseadas em inteligência artificial e biometria comportamental, aumentando a segurança no tratamento de dados, protegendo os titulares e contribuindo para o desenvolvimento de um ambiente digital confiável e competitivo, com total conformidade à LGPD; e
j) Realização de testes e simulações de incidentes.

27. Promover a implementação de políticas robustas para o fortalecimento e expansão de data centers em território nacional, priorizando investimentos em infraestrutura de alta eficiência energética, segurança de dados e integração com redes globais. Essas políticas devem fomentar iniciativas públicas de investimento e parcerias público-privadas nos termos do que fortalece a soberania digital e o interesse popular;

28. Promoção do letramento e da conscientização: garantir disseminação de conhecimento na sociedade acerca do uso de dados pessoais, seus benefícios, riscos e aspectos legais;

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

29. Investimento em educação e capacitação, conscientizando agentes de tratamento e titulares sobre a importância do tratamento adequado de dados pessoais, com transparência e respeito aos direitos dos titulares e demais regramentos estabelecidos pela LGPD, incentivando as práticas legitimas de tratamento de dados pessoais;

30. Desenvolver iniciativas que eduquem os titulares de dados sobre o valor de suas informações pessoais, seus direitos previstos na legislação e as formas de exercê-los;

31. Incentivar a criação de centros de excelência em IA de interesse público e desenvolver programas de capacitação em IA e proteção de dados para profissionais, empreendedores e população em geral são passos importantes para fomentar um ecossistema de inovação que priorize a privacidade e os direitos dos titulares de dados.

32. Promoção do letramento e da conscientização: garantir a disseminação de conhecimento sobre proteção de dados junto a crianças e adolescentes por meio de atuação combinada com outros órgãos da administração como o Ministério da Educação e Ministério dos Direitos Humanos e Cidadania e por meio de parcerias com Estados e Municípios;

33. Proteção de dados na educação: a proteção de dados e a privacidade e os direitos de crianças e adolescentes devem ser priorizados como base em iniciativas tecnológicas no âmbito educacional, devendo as plataformas de *Edtech* garantir conformidade com padrões de privacidade e segurança em relação aos dados estudantis;

34. Incorporar a avaliação de impacto sobre as crianças e adolescentes aos governos em todos os níveis e o mais cedo possível no desenvolvimento de leis e políticas e também serem realizadas pelas companhias no sentido de garantir a sua sustentabilidade empresarial em relação aos direitos de crianças e adolescentes;

35. A construção de uma política nacional integrada, alinhada às melhores práticas globais, é essencial para proteger os direitos dos trabalhadores e fomentar relações laborais mais justas e equilibradas;

36. Promover programas de capacitação para empregadores, gestores e trabalhadores sobre o tratamento responsável de dados pessoais no ambiente laboral;

37. Desenvolver materiais de conscientização voltados aos trabalhadores, destacando seus direitos como titulares de dados e os limites legais do uso de suas informações;

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

38. Incentivar as negociações coletivas para estabelecimento de normas mais específicas para o tratamento de dados pessoais de trabalhadores no contexto laboral, como forma de equilibrar a relação entre empregadores e empregados, estabelecendo salvaguardas claras para proteção dos direitos e liberdades dos trabalhadores, gerando maior segurança jurídica.

Além dos subsídios acima, o Conselheiro Alexandre Boava apresentou itens adicionais, os quais seguem em anexo (Anexo XXX).

De São Paulo para Brasília, 04 de fevereiro de 2025.

Atenciosamente,

RONY VAINZOF:29785203883
RONY VAINZOF:29785203883
2025.02.04 08:45:19 -03'00'

Rony Vainzof
Conselheiro Titular do CNPD e Coordenador do GT 5.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANEXO I – ENTREVISTAS: MIRIAM WIMMER, LUCAS BORGES DE CARVALHO E RENAN KALIL

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ATA DA 4ª REUNIÃO ORDINÁRIA DO GT5 DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE – CNPD

(PORTARIA CNPD Nº 05, DE 4 DE OUTUBRO DE 2024)

1. Dados da Reunião

Data	Horário de início	Horário de término	Local
13/11/2024	8:00H	9:20H	Plataforma Teams

2. Participantes

Rony Vainzof (Coordenador do GT5), Myreilla Pereira, Isabella Henriques, Debora Sirotheau, Alexandre Boava, Vitor Moraes de Andrade, Janaína Lopes (Ministério da Justiça) e Verônica Barros (secretariado). Como especialistas convidados participaram Renan Kalil, Miriam Wimmer e Lucas Borges de Carvalho.

3. Pauta

- Entrevista com especialistas convidados: Renan Kalil, Miriam Wimmer e Lucas Borges de Carvalho.

4. Relato da Reunião

Início:

O Coordenador do GT5, **Rony Vainzof,** procedeu à abertura da reunião, dando boas-vindas ao convidado Renan Kalil e explicou o objetivo do GT5. Miriam Wimmer e Lucas Borges de Carvalho entraram às 8:30h na reunião.

Ref: Entrevista - RENAN KALIL (Ministério Público do Trabalho)
Tema: rotulagem de dados e mercado de trabalho
Dia 13/11/24

Objetivo: apresentar evidências e fornecer subsídios acerca da importância da proteção de dados pessoais para o desenvolvimento econômico, tecnológico e a inovação, para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade (PNPD), conforme fundamento da Lei Geral de Proteção de Dados (LGPD), previsto em seu art. 2º, inc. V;

Entrevistado: Renan Kalil

Professor de Direito no Insper. Doutor e Mestre em Direito pela Universidade de São Paulo. (2019 e 2012). Especialista em Direito Aplicado ao Ministério Público do Trabalho pela Escola Superior do Ministério Público da União (ESMPU). Graduado em Direito com especialização em Direito do Trabalho e da Seguridade Social pela Faculdade de Direito da Universidade de São Paulo (FD-USP).

Renan começou a falar sobre o primeiro ponto: a utilização dos dados pessoais para a compreensão da nova dinâmica em trabalhos menos tradicionais: transporte de pessoas e de mercadorias via plataformas digitais. Há dificuldade sobre a transparência do uso dos dados dos trabalhadores e das empresas (plataformas digitais). O Ministério Público do Trabalho olhou para essa dinâmica para que pudesse melhor compreender essas atividades. O acesso aos dados dessa relação é fundamental, até mesmo para fins de regulação. Comentou sobre uma pesquisa do CEBRAP e sobre a dificuldade de acesso ao resultado dessa pesquisa (apenas os pesquisadores tiveram acesso).

O segundo ponto trazido pelo Renan foi a necessidade de melhor utilização de alguns dispositivos da LGPD para proteção dos interesses dos trabalhadores sobre situações extremamente sensíveis para eles. Se referiu a bloqueios e suspensões no exercício das atividades deles. A forma como esses bloqueios/punições são aplicadas não são transparentes, as empresas apenas dizem que os trabalhadores violaram os Termos de Uso da plataforma. Eles não têm nenhum tipo de conhecimento sobre o que viola os Termos de uso das plataformas. Eles são obrigados a mover ações contra essas empresas para que elas tragam os motivos das punições. É um serviço por elas terceirizado, que utiliza o nome da pessoa, não o CPF para buscas, logo, o trabalhador é frequente punido por um homônimo, mas eles só descobrem isso depois de mover uma ação judicial. O segundo exemplo os bloqueios são oriundos de decisões automatizadas (ex. se não aceitou corridas ou entregas, se a média de nota está abaixo de um padrão). O art. 20 da LGPD diz que as pessoas deveriam ter direito de revisão dessas decisões automatizadas. Dizer que o trabalhador descumpriu os Termos de Uso não atende esse direito. O termo "profissional" do art. 20 não limita a natureza jurídica da relação (como autônomo ou empregado). Entendeu que esse fórum do GT5 era uma ótima oportunidade falar sobre esses temas. Comentou que já há decisões da EU (Holanda – 2 decisões) que usou o art. 22 do GDPR para obrigar algumas empresas (Uber) a darem uma justificativa aos trabalhadores com relação às punições que sofreram.

O terceiro ponto que apresentou: a discriminação nos contratos de trabalho. O uso dos dados pessoais nesse âmbito não é feito de forma condizente com a LGPD. Apresentou três contextos:

(I) Contratação de trabalhadores para desempenhar trabalho nos armazéns: a seleção de currículos usa sistemas de IA, que levam em consideração características da atividade e a experiência da pessoa descrita no currículo. O gênero passou a ter um peso grande para esse trabalho nos armazéns e mulheres deixaram de ser entrevistadas. Isso gerou uma repercussão tão negativa que a empresa deixou de usar esse sistema de IA por conta da discriminação de gênero.
(II) Uso de sistemas de IA para monitoramento dessas atividades dos armazéns: grávidas e pessoas com deficiência passaram a ser punidas por descumprir padrões exigidos de produtividade. Eles foram punidos de forma desproporcional. Grande discussão sobre o uso de sistemas de AI nesses contextos.
(iii) Coworking e plataformas de micro trabalhos. Esclareceu que quando o trabalhador recebe a demanda (treinamento de sistemas de AI), eles não sabem a proveniência do material, o trabalhador não tem a menor ideia de qual será o trabalho final, para o quê aqueles sistemas serão usados. No treinamento de IA os trabalhadores não tem ideia para o quê servirá o sistema que eles estão treinando.

Rony agradeceu a exposição e pediu as fontes dessas pesquisas. Comentou o destaque ao artigo 20 da LGPD nas plataformas digitais. Rony questionou sobre a transparência insuficiente. Mencionou decisão recente sobre o tema no STJ: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2024/15072024-Motorista-de-aplicativo-pode-ser-suspenso-imediatamente-por-ato-grave--mas-plataforma-deve-garantir-defesa.aspx

Débora comentou desconhecer decisão judicial sobre essa opacidade da relação profissional comentada. Pelo que sabe esses casos sempre terminam em acordo. Perguntou se há ou não qualquer decisão judicial nesse sentido. Pediu mais informações sobre o micro trabalho.

Kalil comentou que há algumas decisões sim principalmente na Justiça Comum. Trouxe a ideia dos dispositivos de sistemas de IA que precisam de contextos. Os trabalhadores são treinados com base nas informações e dados que lhe são repassados, mas eles não têm informações sobre a origem das informações e sobre o objetivo do treinamento. Kalil comentou que apresentaria mais material.

Alexandre trouxe o ponto da transparência geral dos dados do trabalhador, nas decisões automatizadas, trouxe a questão da segurança jurídica. Para o Alexandre, transparência ou anonimização das pessoas traria mais segurança jurídica.

Rony sugeriu que talvez um dos pontos principais seria dar efetividade ao §1º, do art. 20, da LGPD:

> *Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (Redação dada pela Lei nº 13.853, de 2019) Vigência*
>
> *§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.*

Fontes citadas:

1) Pesquisa do CEBRAP: https://cebrap.org.br/wp-content/uploads/2023/04/Pocket-Report-AMOBITEC.pdf

2) Decisão do STJ: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2024/15072024-Motorista-de-aplicativo-pode-ser-suspenso-imediatamente-por-ato-grave--mas-plataforma-deve-garantir-defesa.aspx

3) MPT: plataformas digitais: https://mpt.mp.br/pgt/noticias/o-uso-de-dados-pessoais-e-inteligencia-artificial-na-relacao-de-trabalho_web-1.pdf

4) Caso da Holanda. Art. 22 do GDPR. Direito de revisão quando entregadores são bloqueados ou suspensos.

Rony agradeceu a participação de Kalil para a Miriam Wimmer e Lucas de Carvalho iniciarem sua exposição.

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

Ref: Entrevista – Miriam Wimmer (Diretora da ANPD)
Tema: Abordagem Geral
Dia 13/11/24

Objetivo: apresentar evidências e fornecer subsídios acerca da importância da proteção de dados pessoais para o desenvolvimento econômico, tecnológico e a inovação, para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade (PNPD), conforme fundamento da Lei Geral de Proteção de Dados (LGPD), previsto em seu art. 2º, inc. V;

Entrevistada: Miriam Wimmer
Doutora em Políticas de Comunicação e Cultura pela Faculdade de Comunicação da UnB, Mestre em Direito Público e graduada em Direito pela UERJ. Certificada como especialista em proteção de dados pessoais (Europa) pela International Association of Privacy Professionals (CIPP/E).
Bolsista do programa internacional da Universidade de Waseda em Tóquio entre 2001 e 2002, com Distinção Acadêmica. Professora no IDP-Brasília e professora convidada em diversas instituições de ensino de nível superior, em temas relacionados ao direito digital e à proteção de dados pessoais. É servidora pública desde 2007, integrante da carreira de Especialista em Regulação de Serviços Públicos de Telecomunicações da Anatel.
Ocupou diferentes cargos de direção no Ministério das Comunicações - MC e no Ministério de Ciência, Tecnologia, Inovações e Comunicações - MCTIC, onde coordenou a elaboração da Estratégia Brasileira para a Transformação Digital. Desenvolve atividades profissionais e acadêmicas em temas ligados à Internet, às telecomunicações, às políticas digitais e à proteção de dados pessoais.
Currículo lattes: http://lattes.cnpq.br/2365618822386653

Lucas Borges De Carvalho
Gerente de Projetos da Diretora Miriam Wimmer
FORMAÇÃO ACADÊMICA
Possui graduação em Direito pela Universidade Federal da Bahia - UFBA (2003), mestrado em Direito pela Universidade Federal de Santa Catarina - UFSC (2006) e doutorado em Direito pela Universidade de Brasília - UnB (2015).
EXPERIÊNCIA PROFISSIONAL
Procurador Federal da Advocacia-Geral da União desde 2007. Entre outros órgãos públicos, atuou na Consultoria Jurídica do Ministério das Comunicações, na Consultoria Jurídica do

Ministério da Cultura e na Procuradoria Federal Especializada da Anatel. Tem experiência docente, tendo atuado como professor substituto da UFSC e da UnB, entre outras instituições.
INFORMAÇÕES COMPLEMENTARES
Currículo Lattes: http://lattes.cnpq.br/2930035853091994

Rony Apresentou o GT5 e seu objetivo para a Miriam e Lucas.

Miriam comentou da importância do tema do GT5 e ressaltou que a LGPD leva em consideração o desenvolvimento econômico, tecnológico e a inovação (valores constitucionais) como seus fundamentos. A LGPD busca a inovação responsável. Embora não seja uma lei de fomento, entende que traz diretrizes de como os dados devem ser tratados para contribuir para o desenvolvimento econômico, tecnológico e inovação. Trouxe exemplos da consideração desse fato pela ANPD: regulação assimétrica para agentes de pequeno porte. Na época desse regulamento, houve uma preocupação sobre a postura da ANPD de talvez impedir o desenvolvimento econômico. Por isso a preocupação da ANPD em trazer esse regulamento de forma equilibrada para viabilizar o desenvolvimento das atividades desses agentes de forma condizente com a LGPD.

Comentou sobre a Coordenação Geral de Tecnologia e Pesquisa da ANPD. Para ela, ter uma unidade dedicada para esse tema é fundamental para subsidiar os trabalhos da ANPD. Miriam citou o Radar Tecnológico com análises curtas para estimular um debate. Quer proporcionar um debate mais amplo sobre novas tecnologias e sua relação com proteção de dados. Comentou que a ANPD também participa de grupos internacionais, para dar exemplo de conciliação da LGPD e o desenvolvimento tecnológico. Nessa linha de ideia, trouxe o sandbox regulatório, um projeto que está em fase de lançamento. O sandbox é uma ferramenta para obtenção de insumos, que traz de uma forma mais ampla as limitações e possibilidades das tecnologias. Citou a assimetria de informações entre regulador e regulado. O desenvolvimento tecnológico deve vir de mãos dadas com a proteção de dados pessoais (citou o caso Meta e a suspensão do treinamento de IA com dados pessoais pela ANPD) e as abordagens regulatórias mais setoriais ajudam sobre as possibilidades interpretativas da LGPD.

Outro exemplo que evidencia essa a preocupação da ANPD e a relação desenvolvimento e proteção de dados é o Regulamento de Transferência Internacional de Dados. Conversaram com o MDIC (departamento de relações exteriores), que divulgou uma nota técnica com indicadores relevantes que ajudaram a ANPD a dar desenvolver esse Regulamento.

Último ponto trazido pela Miriam: para a promoção da inovação/desenvolvimento é crucial a cooperação da ANPD com outros órgãos públicos. A ANPD não tem por missão institucional desenvolver o país, mas participa de iniciativas do governo no campo da transformação digital, PBIA e seria importante trazer a ANPD como entidade articuladora com outros órgãos públicos que busquem o desenvolvimento tecnológico, econômico e a inovação. Está no papel da ANPD viabilizar o desenvolvimento de políticas públicas de forma condizente com a proteção de dados.

Lucas complementou sobre o papel da ANPD, que tem uma posição privilegiada diante da inovação. É um equilíbrio difícil que deve proporcionar sobre como novas tecnologias se amoldam à regulação e à garantia de direitos. A LGPD traz as condições necessárias para esse equilíbrio ser alcançado. Mencionou sobre segurança jurídica e o documento assinado entre empresas na Europa sobre a falta de segurança jurídica trazendo o GDPR (Disponível em:https://euneedsai.com/). Comentou que vários órgãos de governo que estimulam novas tecnologias, passam por cima da LGPD, por isso ele precisa destacar a importância de participação da ANPD nesses contextos. A compatibilidade entre o uso de novas tecnologias de IA e proteção de dados pessoais é central. Independentemente do que acontecer no PL de IA, a cooperação entre agências é fundamental e precisa ser olhada, já que a LGPD é transversal.

Links compartilhados durante a reunião:

https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2024/15072024-Motorista-de-aplicativo-pode-ser-suspenso-imediatamente-por-ato-grave--mas-plataforma-deve-garantir-defesa.aspx
(Rony)

https://www.gov.br/anpd/pt-br/assuntos/deliberacoes-do-conselho-diretor-1/cds-ano-2023/cd-36-2023-votos.pdf#:~:text=A%20natureza%20jur%C3%ADdica%20do%20Acordo%20entre%20ANPD,I%2C%20e%2084%2C%20VIII%20da%20Constitui%C3%A7%C3%A3o%20Federal
(Miriam)

https://www.gov.br/anpd/pt-br/acesso-a-informacao_antigo/convenios-e-transferencias/acordos-de-cooperacao-internacional (Miriam)

https://euneedsai.com/ (Lucas)

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

Pesquisa do CEBRAP: https://cebrap.org.br/wp-content/uploads/2023/04/Pocket-Report-AMOBITEC.pdf (Rony)

MPT: plataformas digitais: https://mpt.mp.br/pgt/noticias/o-uso-de-dados-pessoais-e-inteligencia-artificial-na-relacao-de-trabalho_web-1.pdf (Rony)

A reunião foi encerrada com o compromisso de o **Rony** enviar os ofícios para as entidades/instituições com solicitações de subsídios para contribuição para os Estudos dos Casos definidos.

Como próximos passos, os Conselheiros definiram que:

- Próxima reunião será dia **21/11;**
- Rony vai enviar ainda esta semana os ofícios para as entidades/instituições indicadas copiando os Conselheiros pertinentes;

A reunião foi encerrada às nove horas e vinte minutos do dia 13 de novembro de 2024.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANEXO II – ENTREVISTA: FABRÍCIO DA MOTA ALVES

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ATA DA ENTREVISTA REALIZADA PELO GT5 DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE – CNPD

(PORTARIA CNPD Nº 05, DE 4 DE OUTUBRO DE 2024)

1. Dados da Reunião

Data	Horário de início	Horário de término	Local
03/12/2024	8:00H	8:53H	Plataforma Teams

2. Participantes

Rony Vainzof (Coordenador do GT5), Myreilla Pereira, Isabella Henriques, Cassio Muniz, Alexandre Boava, Pedro Amaral (Ministério da Justiça) e Verônica Barros (secretariado). Como especialista convidado participou Fabrício da Mota Alves.

3. Pauta

Entrevista: Fabrício da Mota Alves.

Advogado especialista em Direito Digital. Tem vasta experiência na área, tendo participado ativamente no processo legislativo que levou à edição da Lei Geral de Proteção de Dados Pessoais brasileira. Foi assessor legislativo sênior do Senado Federal e participou da Comissão de Juristas que elaborou o projeto de lei de regulação da Inteligência Artificial no Brasil.

Coordenador jurídico da Frente Parlamentar de Proteção de Dados da Câmara dos Deputados. Representante do Senado Federal no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, órgão que compõe a Autoridade Nacional de Proteção de Dados. Professor de Proteção de Dados em São Paulo (Insper, LEC, Escola Paulista de Direito e Opice Blum Academy), Distrito Federal (IDP e ATAME), Paraná (PUC), Rio de Janeiro (FGV) e Recife.

4. Relato da Reunião

Início:

O Coordenador do GT5, **Rony Vainzof,** procedeu à abertura da reunião, dando boas-vindas ao convidado.

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

Fabrício começou a reunião elogiando a abordagem do GT5, porque entende ser importante trazer na Política Nacional de Proteção de Dados e Privacidade a questão da proteção de dados como indutora do desenvolvimento econômico. É sabido que o uso dos dados não pode ser feito sem observar a legislação, mas é preciso ampliar a percepção de tratamento de dados para esse fim. É importante que isso seja refletido na PNPD.

Fabrício comentou sobre a EC 115, impulsionada pelo STF (2021), e ressaltou que sente falta de programas efetivos de valorização da proteção de dados dentro do Governo Federal. Não existe uma campanha pública federal sobre esse tema. A ANPD tem tentado, mas não tem capacidade institucional para ampliar da forma como seria necessária essa conscientização nacional. Qualificar o servidor público em proteção de dados é um problema que precisa ser enfrentado. Embora a ANPD tente, há limitações estruturantes.

Sobre o tema específico de desenvolvimento econômico e inovação responsável, Fabrício comentou sobre o "Privacy by Design", uma ferramenta que acaba influenciando instituições públicas e privadas. Logo, para ele a implementação da proteção de dados e privacidade by design é relevante para impulsionar esse desenvolvimento. Comentou que o desenvolvimento de programas de educação e de promoção de incentivos à conformidade também precisam ser implementados pelo governo. Proteção de dados é um tema que deve estar presente em todas as iniciativas do Estado, que também deve estimular as empresas privadas a ter transparência, tudo com o objetivo de estabelecer uma relação de confiança com os indivíduos. A necessidade de se planejar regulações flexíveis e adaptáveis, de se ter um diálogo responsável é de extrema importância. A ANPD já tem trazido essa flexibilidade. A punição deve ser a *ultima ratio* e a colaboração do administrado é imprescindível (regulação responsiva). Ademais, é preciso se espelhar nos exemplos internacionais, onde já há um melhor equilíbrio com proteção de dados e desenvolvimento. A ANPD tem que participar de todos esses debates nas relações internacionais que tratam do tema, mas isso deve se espraiar para outros órgãos, como Ministério das Relações Exteriores.

Fabrício trouxe a necessidade de diálogo entre os entes federativos, uma vez que eles precisam de um apoio do Governo Federal.

No âmbito de uma PNPD não devemos nos preocupar com a regulação, mas sim com as diretrizes e limites que serão dados para a atuação do Estado Brasileiro como um todo. É essa a visão que se deve ter para a PNPD.

Fabrício comentou que sempre criticou a falta de informação, de dados que pudesse dar um diagnóstico exato da sociedade brasileira. Ele comentou de uma pesquisa que seu escritório fez em empresas de capital aberto e notou a eficácia desse instrumento, mas disse que não há essas iniciativas pelo Estado. Na sociedade civil essa inciativa existe e deve ser estimulada. Trouxe uma preocupação pessoal sobre esse

tema e incentivou a necessidade de as pesquisas envolverem crianças e adolescentes. Comentou sobre a falha de educação parental, pois os pais não têm controle do que os filhos acessam na internet.

A reunião foi encerrada às oito e cinquenta e três minutos do dia 03 de dezembro de 2024.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANEXO III – ENTREVISTAS: FABRÍCIO GUIMARAES MADRUGA LOPES E FABIANA SILVA PINTO FARACO CEBRIAN

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ATA DA ENTREVISTA REALIZADA PELO GT5 DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE – CNPD

(PORTARIA CNPD Nº 05, DE 4 DE OUTUBRO DE 2024)

1. Dados da Reunião

Data	Horário de início	Horário de término	Local
13/12/2024	8:00H	9:00H	Plataforma Teams

2. Participantes

Rony Vainzof (Coordenador do GT5), Myreilla Pereira, Isabella Henriques, Alexandre Boava, Debora Sirotheau e Pedro Amaral (Ministério da Justiça). Como especialistas convidados participaram Fabricio Madruga e Fabiana Cebrian.

3. Pauta

- Entrevista com **Fabricio Madruga** e **Fabiana Cebrian**.

4. Relato da Reunião

Início:

O Coordenador do GT5, **Rony Vainzof,** procedeu à abertura da reunião, dando boas-vindas aos convidados e explicou o objetivo do GT5.

Fabiana Silva Pinto Faraco Cebrian:

- Sugestão para a inclusão de um campo de definições na PNPD, com o objetivo de diferenciar termos como "automatização" e "automação", exemplificando com o Artigo 20 da LGPD.
- Debate sobre a saída de modelos de aprendizado de máquina, exemplificando com a análise de crédito, e a necessidade de discutir quem define os critérios para decisões com base em probabilidades.
- Interesse no tema "cidades inteligentes", presente no e-mail do GT5.
- Discussão sobre a proliferação de sensores em ambientes urbanos e residenciais, e a necessidade de discutir a coleta de dados, privacidade e vigilância nesse contexto.

- Tendência de uso de dados de sensores para direcionamento de anúncios, exemplificando com o caso de eletrodomésticos.
- Preocupação com a coleta de dados por softwares de gestão de placas solares, dada a popularização de carros elétricos e a conexão das placas à rede residencial.
- Sugestão para a criação de normas de interoperabilidade entre diferentes aplicativos e dispositivos, visando a análise do fluxo de dados e a proteção de dados pessoais.
- Necessidade de diretrizes para o contexto atual de uso de dados pessoais.
- Sugestão de incentivos para a inovação responsável, por meio da criação de sandboxes regulatórios com foco em IA e cidades inteligentes.
- Criação de mecanismos de certificação em proteção de dados.

Fabricio Guimaraes Madruga Lopes:
- Importância de se trabalhar a proteção de dados em conjunto com a segurança digital, evitando o descuido com a proteção de dados em nome da segurança.
- Relevância do tema "autenticação e identificação digital", presente na lista de tópicos do GT5.
- Importância de se investir em soluções tecnológicas para o ambiente digital.
- Diferenciação entre "prevenção à fraude" e "proteção ao crédito", destacando que a proteção ao crédito se limita à capacidade de pagamento, enquanto a prevenção à fraude envolve a verificação da identidade e da veracidade das informações.
- A LGPD como um marco regulatório para a proteção de dados no Brasil, em contraste com a legislação anterior, que tratava do tema de forma isolada.
- A LGPD como um fomentador de pesquisa e desenvolvimento de novas soluções, em virtude das obrigações que impõe.
- Relação entre a LGPD e a estratégia de governo digital do Brasil, com foco na criação de um ambiente seguro para transações comerciais no ambiente digital.
- A proteção de dados como essencial para a oferta de serviços como identificação, proteção ao crédito e prevenção à fraude de forma sustentável e respeitosa aos direitos fundamentais.
- A importância de limites para a coleta e uso de dados, com base nos princípios da LGPD, para evitar a coleta desenfreada de dados e a criação de um ambiente hostil para os titulares.
- A necessidade de se comunicar a importância da proteção de dados para a criação de um ambiente seguro para transações, e para a sustentabilidade do desenvolvimento tecnológico.
- A LGPD como um marco para a formalização da preocupação com a segurança da informação no Brasil, e a relação intrínseca entre segurança da informação e proteção de dados.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

- A necessidade de se destacar a relação entre segurança da informação e proteção de dados na PNPD.
- O uso intenso de dados pessoais como um requisito para o desenvolvimento no ambiente digital.
- Os dados pessoais como insumo para gerar valor em áreas como segurança, identificação e proteção ao crédito, mas também como a própria riqueza a ser explorada de forma responsável.
- Exemplo da coleta de dados de eletrodomésticos para otimizar o consumo de energia, e a necessidade de se encontrar um equilíbrio entre os benefícios e os riscos à privacidade.
- A LGPD como um marco regulatório seguro para investimentos em atividades que envolvam o uso de dados pessoais.
- Oportunidade para o Brasil se desenvolver a partir da exploração responsável da "riqueza" de dados pessoais gerada por sua população.

A reunião foi encerrada às 9h00.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANEXO IV – ENTREVISTAS: RODRIGO SANTANA DOS SANTOS E EDUARDO GOMES SALGADO

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ATA DA ENTREVISTA REALIZADA PELO GT5 DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE – CNPD

(PORTARIA CNPD Nº 05, DE 4 DE OUTUBRO DE 2024)

1. Dados da Reunião

Data	Horário de início	Horário de término	Local
13/12/2024	11:00H	12:00H	Plataforma Teams

2. Participantes

Rony Vainzof (Coordenador do GT5), Myreilla Pereira, Alexandre Boava e Pedro Amaral (Ministério da Justiça). Como especialistas convidados participaram Rodrigo Santana e Eduardo Gomes.

3. Pauta

- Entrevistas: **Rodrigo Santana** e **Eduardo Gomes**.

Rodrigo Santana dos Santos - Coordenador-Geral de Normatização da ANPD

Eduardo Gomes Salgado - Coordenador-Geral de Relações Institucionais e Internacionais da ANPD

4. Relato da Reunião

Início:

O Coordenador do GT5, **Rony Vainzof,** procedeu à abertura da reunião, dando boas-vindas aos convidados e explicou o objetivo do GT5.

Rodrigo Santana

Modelo Regulatório:

- Sistema que visa fortalecer o desenvolvimento, observando os riscos à proteção de dados.

- Destaca a transparência, estabilidade e previsibilidade como características do processo regulatório, exemplificando com a Agenda Regulatória, que define os temas prioritários de atuação da ANPD.
- Ressalta a importância da Análise de Impacto Regulatório (AIR) como ferramenta para avaliar as intervenções regulatórias e minimizar os impactos negativos sobre os agentes econômicos e a sociedade.
- Menciona a necessidade de fortalecer a equipe da ANPD e adotar boas práticas internacionais para a realização de AIRs robustas e baseadas em dados.
- Destaca o Sandbox Regulatório como um instrumento de inovação que permite a experimentação de novas tecnologias e modelos de negócio em um ambiente controlado, com a participação da ANPD.
- Enfatiza a necessidade de fortalecer a ANPD institucionalmente para garantir a segurança jurídica aos agentes econômicos e a efetividade da LGPD.
- O fortalecimento da ANPD é fundamental para a promoção da inovação e do desenvolvimento, pois garante estabilidade e previsibilidade regulatória.
- Lista alguns pontos que justificam o fortalecimento da ANPD:

Ações Educativas: criação de uma área dedicada a ações educativas para promover a cultura de proteção de dados no país.

Comunicação: criação de uma assessoria de comunicação para melhorar a comunicação da ANPD com a sociedade.

Assessoria Parlamentar: criação de uma assessoria parlamentar independente para fortalecer a interlocução da ANPD com o Legislativo.

- Destaca a importância da atuação institucional da ANPD em parceria com outras agências reguladoras, ministérios e entidades relevantes, como o Ministério das Relações Exteriores e o MDIC.
- Necessidade de fortalecer a cooperação com o setor privado e a sociedade civil, por meio de instrumentos como os Acordos de Cooperação Técnica (ACTs) e o Fórum de Comunicação Permanente previsto na LGPD.
- Desafios setoriais da proteção de dados e a Agenda Regulatória da ANPD.

Material resumido disponibilizado pelo Rodrigo dos pontos relevantes:

- Fortalecimento de boas práticas regulatórias;
- Agenda Regulatória como instrumento de previsibilidade e segurança jurídica;
- Análise de Impacto Regulatório como instrumento regulatório de análise de impacto da intervenção regulatória aos agentes de tratamento e titulares;
- Aprimoramento do processo de monitoramento regulatório (Avaliação de Resultado Regulatório e Monitoramento do Ambiente Regulado);
- Fortalecimento institucional da ANPD;

- Aprimoramento do processo de Ações Educativas;
- Ações regulatórias e educativas articuladas com outras entidades públicas;
- Aprimoramento de instrumentos regulatórios para fomentar a inovação, como por exemplo o Sandbox Regulatório;
- Atuação regulatória alinhada às questões internacionais;
- Aprimorar a estratégia de uso de dados, informações e evidências nas tomadas de decisões regulatórias da ANPD.

Eduardo Gomes Salgado

- Destaca a busca por uma aproximação com outras agências reguladoras, com a assinatura de ACTs em andamento.
- Importância da institucionalização de eventos da ANPD, como o Encontro de Encarregados e a comemoração dos 4 anos da agência.
- Descreve a atuação internacional da ANPD, com destaque para a participação em fóruns globais como o Global Privacy Assembly (GPA) e a Rede Ibero-americana de Proteção de Dados.
- Menciona a aprovação do Regulamento de Transferência Internacional de Dados e a importância das decisões de adequação em curso com a União Europeia e o Reino Unido para o desenvolvimento econômico e tecnológico.
- Reforça a necessidade de fortalecer a ANPD institucionalmente, mencionando a perda de servidores qualificados nos últimos meses.
- Argumenta que o fortalecimento da ANPD é fundamental para que a agência possa atuar de forma eficaz na regulação da inteligência artificial, considerando a eventual aprovação do PL 2338.
- Defende a necessidade de investimentos em infraestrutura, pessoal e orçamento para garantir a capacidade de atuação da ANPD.
- Destaca a importância da atuação em parceria com outras agências reguladoras, ministérios e entidades como o MDIC.
- Menciona a necessidade de estreitar o diálogo com o setor privado, por meio de iniciativas como os encontros com o Conselho de Defesa do Consumidor (CDR).

A reunião foi encerrada às 12h00.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANEXO V – ENTREVISTA: RONALDO LEMOS

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ATA DA ENTREVISTA REALIZADA PELO GT5 DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE – CNPD

(PORTARIA CNPD Nº 05, DE 4 DE OUTUBRO DE 2024)

1. Dados da Reunião

Data	Horário de início	Horário de término	Local
12/12/2024	14:00H	14:30H	Plataforma Teams

2. Participantes

Rony Vainzof (Coordenador do GT5), Myreilla Pereira, Isabella Henriques, Alexandre Boava, Fabio Souza, Pedro Amaral (Ministério da Justiça) e Verônica Barros (secretariado). Como especialista convidado participou Ronaldo Lemos.

3. Pauta

- Entrevista com especialista convidado: Ronaldo Lemos.

4. Relato da Reunião

Início:

O Coordenador do GT5, **Rony Vainzof,** procedeu à abertura da reunião, dando boas-vindas ao convidado e explicou o objetivo do GT5.

Ref. Entrevista RONALDO LEMOS

Dia 12/12/2024

Objetivo: apresentar evidências e fornecer subsídios acerca da importância da proteção de dados pessoais para o desenvolvimento econômico, tecnológico e a inovação, para a elaboração da Política de Proteção de Dados Pessoais e da Privacidade (PNPD), conforme fundamento da Lei Geral de Proteção de Dados Pessoais, previsto em seu art. 2º, inc.V.

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

Ronaldo é Mestre em Direito pela Universidade de Harvard e doutor pela USP, Ronaldo Lemos é professor da Universidade de Columbia, colunista do jornal Folha de S. Paulo, da revista Trip e da Globonews. Além disso, é um dos criadores do Marco Civil da Internet, lei que regula o uso da internet no Brasil, aprovada em 2014. Reconhecido internacionalmente por ser especialista em temas como tecnologia, dados, mídia e propriedade intelectual.

Ronaldo Lemos iniciou sua fala destacando um primeiro ponto sobre a função da LGPD e da mudança de paradigma que ela trouxe. Diferentemente da Europa, que já tinha leis de proteção de dados há décadas e depois veio o GDPR para aperfeiçoar o modelo, o Brasil iniciou a discussão do tema com a LGPD. A transição que ocorreu no Brasil foi brusca e apresentou uma abrangência maximalista. É preciso lembrar da função da LGPD para evitar as armadilhas do maximalismo. Comentou sobre Claudio Weber Abramo, sobre o perigo do mal uso interpretativo da LGPD no sentido de limitar a transparência, em especial da atuação da administração pública (Lei de Acesso à Informação) e de políticas públicas[5]. E de certa forma isso ocorreu, mas esse maximalismo distorce a LGPD. Lei de Proteção de Dados Pessoais não é feita para trancar o dado, mas sim para permitir que o dado circule. Segundo Ronaldo, embora pareça paradoxal é isso mesmo, o dado pode e deve circular, ele pode gerar valor, desenvolvimento econômico. Não se pode confundir proteção de dados com sigilo, o que ele costuma ver com frequência. A LGPD gerou alguns desequilíbrios. A ANPD tem que atuar, tem que proteger dados pessoais, mas tem também que permitir geração de valor a partir do tratamento e da circulação dos dados, desde que seja de forma lícita. E a LGPD traz esses parâmetros. A LGPD tem dois objetivos: proteção de direitos e fomento ao desenvolvimento econômico, geração de riqueza. No Brasil temos visto um movimento apenas para a proteção de direitos, e estamos esquecendo do outro lado, da geração de riqueza. A LGPD pode sim ser a base do desenvolvimento econômico, desde que o tratamento de dados seja lícito. Um segundo ponto que ele trouxe diz respeito à autonomia da ANPD que, de forma institucional, precisa estabelecer uma relação mais independente com relação ao Poder Executivo. A ANPD surgiu dependente do Executivo, agora ganhou um pouco de autonomia, mas essa autonomia é limitada, pois depende do Ministério da Justiça, depende se servidores de outros Ministérios. Com o avanço do PL de IA, no qual a ANPD recebe mais poderes, é preciso estabelecer, de forma clara, que a ANPD é uma autoridade independente do poder político. Essa é uma agenda essencial para evitar descarrilamento das funções da Autoridades. Terceiro ponto, sobre IA, comentou que entregar a gestão para a ANPD é extremamente problemático por conflito de interesses. Proteção de dados e regulação da IA são temas conflitantes. Há conflitos insolúveis nessa

[5] https://www.poder360.com.br/opiniao/lei-de-protecao-de-dados-ameaca-acesso-a-informacao-diz-claudio-w-abramo/ e https://itsrio.org/pt/artigos/lei-de-protecao-de-dados-esta-sendo-usada-contra-transparencia/.

relação. De acordo com Ronaldo, a ANPD deveria resistir a assumir a essa função, pois perde a proteção de dados e perde a regulação de IA. Por fim, último ponto que abordou se referiu à pauta da ANPD que deveria ser mais inclusiva. Ela tem atuado em questões extremamente relevantes, porém com foco em Big Techs. Segundo ele, o problema de proteção de dados no Brasil é muito mais profundo, pois há outras questões mais urgentes e abrangentes que não estão recebendo tanta atenção, como o grande vazamento de dados dos brasileiros (escreveu artigo na Folha sobre isso). O Brasil se tornou um paraíso de golpes. Citou o golpe de Whatsapp. Comentou que os idosos são os mais explorados. A realidade é caótica e não tem ninguém protegido. Comentou que a ANPD poderia dar mais atenção ao tema. Esse problema afeta 100% das pessoas nesse país, especialmente as mais vulneráveis.

Ronaldo comentou que é favorável a banir celular nas escolas, de liberação da rede social só a partir dos 13 anos. Por outro lado, ressaltou que o acesso à informação muda vidas. Para ele, as pessoas precisam lembrar que é possível aprender qualquer coisa de graça na internet. O Brasil é um país muito pobre e as pessoas têm dificuldade de acesso a habilidades disponíveis. É importante ampliar o acesso ao conhecimento, a habilidades (*skills)* que muda a vida, mas o desafio é o que o ALANA tenta fazer. Como proteger as crianças e adolescentes desse "canto das sereias" e levá-los para esse campo de acesso que podem transformar vidas.

A reunião foi encerrada às catorze horas e trinta e dois minutos do dia 12 de dezembro de 2024.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANEXO VI – CONTRIBUIÇÕES: ASSOCIAÇÃO BRASILEIRA DE EMPRESAS DE SOFTWARE (ABES)

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ABES associação brasileira das empresas de software

São Paulo, 02 de dezembro de 2024.

Ao
Ilmo. Sr. **Rony Vainzof**
Conselheiro Titular do CNPD e coordenador do GT 5

REF.: Solicitação de contribuição ao CNPD (GT5)

Prezado Rony Vainzof,

A **ABES** - Associação Brasileira de Empresas de Software, sediada Av. Ibirapuera, 2907 – 8º and – Cj 811 - CEP 04029-200 - São Paulo - S.P. Fone: (11) 5094-3100, é uma **Entidade de Classe Empresarial, a nível nacional,** com abrangência em todo o Território da República Federativa do Brasil, que congrega em seu quadro associativo cerca de 2.000 (duas mil) empresas associadas/conveniadas, que totalizam, aproximadamente, 85% do faturamento do setor de software e serviços no Brasil, distribuídas em 24 Estados e Distrito Federal, responsáveis pela geração de mais de 260 mil empregos diretos e um faturamento anual da ordem de R$ 107 bilhões em 2023, dados que habilitam a Entidade como legítima representante de enorme parcela das empresas de **SOFTWARE** e Serviços Técnicos Complementares que operam no Brasil.

A entidade tem com o propósito contribuir para a construção de um Brasil Mais Digital e Menos Desigual, pois acredita que a tecnologia da informação desempenha um papel fundamental para a democratização do conhecimento e a criação de novas oportunidades, visando melhor qualidade de vida para todos, de forma inclusiva e igualitária. Diante desse propósito, o objetivo da ABES é o de assegurar um ambiente de negócios propício à inovação, ético, dinâmico, sustentável e competitivo globalmente. Desde sua fundação, em setembro de 1986, a ABES busca ser relevante para seus associados e referência nacional e internacional do setor de tecnologia, participando ativamente da revolução promovida pela transformação digital, promovendo o empreendedorismo e a inovação, reivindicando políticas públicas para a construção de um modelo setorial forte, estrategicamente adequado à realidade global e com segurança jurídica.

Em atendimento ao ofício recebido, o Grupo de Trabalho de Proteção de Dados da ABES, **liderado por Daniella Caverni e Francisco Espuny**, elaborou contribuições sobre a temática de dados pessoais como motor para o desenvolvimento econômico, tecnológico e a inovação. Essas contribuições visam colaborar na construção da Política Nacional de Proteção de Dados Pessoais e da Privacidade, sob a coordenação do Conselho Nacional de Proteção de Dados.

abesrelacionamento@abes.org.br | www.abes.org.br
Av. Ibirapuera - 2907 - 8º Andar - Cj 811 - Moema
São Paulo - SP - CEP: 04029 - 200
Telefone: + 55 11 2161 - 2833

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ABES associação brasileira das empresas de software

1) **Casos práticos e dados estatísticos que demonstrem a importância do uso e da proteção de dados pessoais para o desenvolvimento econômico, tecnológico e a inovação;**

Não se pode falar de desenvolvimento econômico, tecnológico e inovação e não tratar da importância dos dados pessoais, já que se trata de um ativo essencial nestes processos.

A privacidade não é apenas um direito fundamental do cidadão, , mas também um elemento estratégico que determina a forma como a sociedade lida com a tecnologia, inovação e governança. Nesse contexto a proteção de dados pessoais desempenha um papel crucial ao incentivar práticas empresariais responsáveis e éticas, conforme orientado pela LGPD, promovendo os seguintes pilares:

1. **Inovação responsável:** Empresas e desenvolvedores de tecnologia passam a criar soluções mais seguras, pensando em privacidade e proteção de dados desde a concepção, promovendo a uma relação de confiança com o consumidor e aumentando sua competitividade no mercado.

2. **Governança transparente:** Políticas públicas e marcos regulatórios que priorizam a proteção de dados fortalecem o equilíbrio entre avanço tecnológico e respeito aos direitos individuais.

3. **Empoderamento do cidadão:** O controle ativo sobre seus próprios dados permite que indivíduos exerçam seus direitos de forma mais consciente, moldando como as instituições respondem às suas demandas.

4. **Sustentabilidade social e digital:** Um ambiente digital com privacidade robusta favorece a inclusão, reduz desigualdades e estimula relações mais éticas entre os diferentes agentes da sociedade.

Esses fatores refletem como o futuro da privacidade está intrinsecamente ligado à evolução tecnológica, à governança global e aos valores éticos da sociedade. Para empresas de tecnologia, alinhar inovação com proteção de dados é uma estratégia não apenas para conformidade legal, mas também para criação de valor e diferencial competitivo.

abesrelacionamento@abes.org.br | www.abes.org.br
Av. Ibirapuera - 2907 - 8º Andar - Cj 811 - Moema
São Paulo - SP - CEP: 04029 - 200
Telefone: + 55 11 2161 - 2833

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ABES associação brasileira das empresas de software

Conforme o estudo "*Mercado Brasileiro de Software: Panorama e Tendências 2024*", uma iniciativa da ABES – Associação Brasileira das Empresas de Software e da consultoria IDC[1], mais de 90% das empresas de grande porte no Brasil já utilizam IA em seus processos, destacando sua importância para inovação. A aplicação da IA é chave para criar soluções personalizadas e aumentar a competitividade.

De acordo com esse mesmo estudo: "*Em 2023, o mercado de programas de computador desenvolvidos no País (incluindo aí o software sob encomenda e as exportações) representou aproximadamente 34,8% do investimento total, confirmando o aumento na tendência de participação do software desenvolvido no País em relação ao mercado total, tendência esta que vem sendo apontada desde o início deste estudo".*

O mercado de *cloud* segue em franca expansão, representando um total de US$ 1,5 bilhão em 2024 no Brasil. Em 2024, o universo de dados no mundo ultrapassará 157 ZB, podendo dobrar até 2027. Quase 25% desse volume já está na nuvem, que cresce com o dobro da velocidade em relação ao que não está em Cloud, com especial destaque para Aplicações Colaborativas, Aplicações de CRM e Aplicações de Conteúdo. Já no segmento de IoT, incluindo hardware de conectividade, software e serviços, o mercado também cresceu, com uma taxa de 20,2% em relação ao ano de 2021.

Conforme apurado, para que esses dados possam ser utilizados para a geração de inteligência e valor para os negócios, muitas companhias acelerarão e aprimorarão sua estratégia de dados. Para 55% das empresas, criar produtos e serviços, aumentar a capacidade personalizada e gerar novas fontes de receitas são temas estratégicos que dependem fortemente do uso eficaz dos dados pessoais e não pessoais.

Ademais, para lidar com o crescente volume de dados, os investimentos em soluções na nuvem para Data Management, Analytics e AI/ML serão ampliados. A Integração e interoperabilidade em ambientes híbridos e multicloud serão essenciais para garantir que os dados estejam disponíveis e possam ser efetivamente utilizados de forma ética e legal e as áreas de negócio, por sua vez, esperam respostas mais rápidas e com mais insights. Para isso, terão que trabalhar em parceria com a TI no amadurecimento da cultura de dados, que será possível com treinamentos e entendimento a legislação e resoluções publicadas pelos órgãos oficiais.

[1] https://abes.com.br/dados-do-setor/

abesrelacionamento@abes.org.br | www.abes.org.br
Av. Ibirapuera - 2907 - 8º Andar - Cj 811 - Moema
São Paulo - SP - CEP: 04029 - 200
Telefone: + 55 11 2161 - 2833

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ABES associação brasileira das empresas de software

2) Como a LGPD e outras normas aplicáveis, nacionais e internacionais, servem como bússola para que os dados pessoais possam ser utilizados para o desenvolvimento econômico, tecnológico e a inovação, de forma ética, segura e responsável?

A LGPD deve ser considerada como um importante pilar para o desenvolvimento de um futuro digital sustentável e inovador, já que garante e orienta o tratamento dos dados pessoais por todos os entes públicos e/ou privados por meio de seus princípios, governança e bases legais. Com isso, o ambiente passou a contar com diretrizes claras e respeitosas para o tratamento dos dados pessoais em todos os setores da economia, o que trouxe acima de tudo, segurança jurídica para o desenvolvimento econômico, tecnológico e, como consequência, para a promoção da inovação.

A LGPD garante equilíbrio entre o uso dos dados pessoais e a inovação tecnológica, já que traz princípios e bases legais específicas para o tratamento dos dados, ou seja, o avanço tecnológico poderá ser conduzido de forma ilimitada, desde que respeitadas essas diretrizes com a utilização dos dados pessoais de forma ética e responsável.

O cumprimento da LGPD não é apenas uma obrigação legal, mas uma oportunidade estratégica para conquistar a confiança de clientes e parceiros. Empresas que implementam medidas de boas práticas em proteção de dados ganham credibilidade no mercado que, por sua vez, estimula o compartilhamento consciente de informações, gerando insights valiosos que impulsionam a inovação e criam novas oportunidades de negócio. Ademais, empresas que efetivamente cumprem a LGPD não apenas garantem conformidade com a legislação brasileira, mas também conquistam uma vantagem competitiva ao se posicionarem como confiáveis no cenário global.

A LGPD incentiva o desenvolvimento de tecnologias que integrem a proteção de dados desde o início do projeto, tornando a privacidade um elemento padrão. Isso promove a criação de ferramentas seguras, como sistemas de anonimização, criptografia e modelos federados de IA. A regulamentação exige que as empresas repensem processos e invistam em inovação para atender também às normas. Isso resulta em tecnologias mais avançadas, seguras e confiáveis.

A LGPD trouxe como fator basilar ao tratamento dos dados pessoais o princípio da transparência, portanto, a LGPD exige que empresas sejam transparentes sobre como utilizam os dados, promovendo práticas éticas e responsáveis. Isso reduz o risco de manipulação de dados ou discriminação algorítmica, criando um ambiente mais justo e seguro para o mercado. Normas como a LGPD exigem que algoritmos sejam transparentes e explicáveis, incentivando o desenvolvimento de IA ética, que respeite direitos e evite discriminação.

abesrelacionamento@abes.org.br | www.abes.org.br
Av. Ibirapuera - 2907 - 8º Andar - Cj 811 - Moema
São Paulo - SP - CEP: 04029 - 200
Telefone: + 55 11 2161 - 2833

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ABES associação brasileira das empresas de software

A obrigatoriedade de avaliar os riscos no uso de dados, por meio de relatórios de impacto à proteção de dados, previne abusos e orienta o uso responsável de informações. Isso é especialmente relevante para tecnologias sensíveis, como IA e IoT, onde o mau uso de dados pode trazer consequências imprevisíveis. Normas como a LGPD obrigam as empresas a implementarem medidas técnicas e organizacionais robustas para proteger dados, fortalecendo a segurança digital e prevenindo vazamentos.

A LGPD representa um marco essencial para o desenvolvimento de um futuro digital sustentável, equilibrando a proteção de dados pessoais com o avanço tecnológico. Ao exigir práticas transparentes, éticas e responsáveis, a LGPD se torna um catalisador para tecnologias mais seguras e avançadas, fomentando um ambiente que respeita direitos fundamentais e promove o crescimento econômico, tecnológico e inovador.

Em um mundo completamente conectado, a conformidade com a LGPD é mais do que uma obrigação legal; é uma oportunidade estratégica para empresas e organizações públicas se posicionarem como líderes na construção de uma sociedade ética e inovadora. A LGPD posiciona o Brasil como um protagonista global ao alinhar-se a regulações internacionais como o GDPR da União Europeia. Essa harmonização facilita parcerias transnacionais e fomenta a competitividade das empresas brasileiras em mercados globais. O respeito a normas globais de proteção de dados aumenta a atratividade de empresas brasileiras para investimentos estrangeiros e parcerias tecnológicas.

3) Quais práticas poderiam ser implementadas para melhorar a proteção de dados e segurança jurídica no tratamento de dados pessoais para o desenvolvimento econômico, tecnológico e a inovação?

O papel do Estado no financiamento e estímulo ao desenvolvimento de soluções tecnológicas voltadas para inovação e tratamento responsável de dados pessoais é crucial para alavancar a competitividade do setor privado e garantir a proteção de dados no Brasil. Ele pode ser dividido em diversas frentes, incluindo incentivos financeiros, apoio regulatório e estímulos à cooperação público-privada.

Muitas são as práticas que podem ser implementadas para melhorar a proteção de dados e a segurança jurídica no tratamento de dados pessoais para o desenvolvimento econômico, tecnológico e inovação.

abesrelacionamento@abes.org.br | www.abes.org.br
Av. Ibirapuera - 2907 - 8º Andar - Cj 811 - Moema
São Paulo - SP - CEP: 04029 - 200
Telefone: + 55 11 2161 - 2833

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ABES associação brasileira das empresas de software

Vamos iniciar esta análise com a necessidade de se garantir segurança jurídica, que é essencial para empresas que desejam inovar com responsabilidade. Garantir que a LGPD seja interpretada de maneira uniforme em diferentes setores reduz ambiguidades e conflitos legais, criando um ambiente mais previsível e favorável para o desenvolvimento tecnológico

Quando as regras e exigências são claras e aplicadas de forma consistente, tanto as empresas quanto os desenvolvedores de tecnologia e investidores encontram um ambiente mais previsível e favorável para criar, testar e lançar novas soluções.

A publicação de guias e orientadores pelos órgãos reguladores, como a ANPD, é uma prática que fortalece esta interpretação, além da realização de campanhas de conscientização e capacitação técnica para empresas e instituições públicas.

Ademais, uma interpretação segura e uniforme nos leva ao segundo ponto que entendemos como uma prática fundamental no tratamento dos dados pessoais para o desenvolvimento econômico, tecnológico e a inovação: **a harmonização da legislação com as principais regras e padrões internacionais de tratamento de dados pessoais**.

Uma interpretação uniforme alinhada a padrões internacionais, como o GDPR, reduz barreiras para empresas brasileiras que desejam competir globalmente, promovendo a exportação de tecnologia e serviços, a aceitação de que a transferência internacional de dados possa ser efetuada com base nas regras já estabelecidas por outros mercados que atendem aos diretos fundamentais de proteção de dados traz competitividade e evita burocratização, ampliando o alcance comercial das empresas locais, estimulando o desenvolvimento de novas tecnologias e trazendo mais competitividade para a economia.

Regras consistentes simplificam processos de aprovação para novos projetos, permitindo que inovações sejam lançadas mais rapidamente.

Incentivos econômicos e tecnológicos podem também ser uma excelente prática para fomentar o desenvolvimento econômico, tecnológico e a inovação. Neste sentido entendemos que podem ser considerados incentivos:

- Conceder isenções fiscais ou benefícios para empresas que implementem boas práticas de proteção de dados ou desenvolvam tecnologias que respeitem a privacidade (privacy by design);

abesrelacionamento@abes.org.br | www.abes.org.br
Av. Ibirapuera - 2907 - 8º Andar - Cj 811 - Moema
São Paulo - SP - CEP: 04029 - 200
Telefone: + 55 11 2161 - 2833

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ABES associação brasileira das empresas de software

- Fomentar a pesquisa e desenvolvimento (P&D) com o financiamento de projetos de inovação tecnológica voltados à segurança da informação.
- Estimular escolas e universidades a incluírem temas como LGPD, ética digital e governança de dados em seus currículos.
- Criar iniciativas para reconhecer empresas e instituições que integram privacidade e proteção de dados em seus modelos de negócios de forma inovadora.
- Revisar periodicamente a LGPD e/ou regulamentos para acompanhar o avanço tecnológico, como o surgimento de IA generativa, IoT e blockchain.
- Criar programas nacionais para fortalecer a segurança digital, com ênfase em proteger infraestruturas críticas e redes públicas.
- Oferecer plataformas de segurança gratuitas ou de baixo custo para pequenas e médias empresas (PMEs), como sistemas de criptografia e monitoramento de segurança.
- Estabelecer parcerias entre governos, empresas e organizações não governamentais para desenvolver políticas e tecnologias de proteção de dados.
- Criar fóruns ou conselhos regionais para promover o intercâmbio de ideias e estratégias entre setores.
- Promover diretrizes que exijam transparência e equidade em algoritmos de inteligência artificial, evitando vieses e discriminação.

Assim, entendemos que a harmonização das regras de proteção de dados com padrões internacionais, como o GDPR, fortalece a competitividade do Brasil no mercado global, permitindo que empresas locais inovem e ampliem seu alcance comercial de forma segura.

Incentivos econômicos e educacionais, como benefícios fiscais, financiamento de pesquisas e inclusão de temas sobre privacidade e ética digital nas escolas, são fundamentais para estimular a inovação tecnológica e preparar a sociedade para o futuro digital.

abesrelacionamento@abes.org.br | www.abes.org.br
Av. Ibirapuera - 2907 - 8º Andar - Cj 811 - Moema
São Paulo - SP - CEP: 04029 - 200
Telefone: + 55 11 2161 - 2833

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ABES associação brasileira das empresas de software

Além disso, parcerias entre governos, empresas e organizações promovem soluções mais eficazes e seguras, enquanto diretrizes claras e consistentes reduzem burocracias e aceleram o desenvolvimento de novos projetos. Com essas ações, o Brasil pode construir um ambiente econômico e tecnológico mais forte, ético e conectado às demandas globais, garantindo a proteção dos dados pessoais.

Implementação e reconhecimento de códigos de conduta setoriais, que podem ser reconhecidos por autoridades públicas, também representam importantes instrumentos regulatórios, de forma a absorver melhor incertezas e desenvolver parâmetros consolidados de eficácia legal mediante a atuação de organizações especializadas nas práticas do seu respectivo setor. Exemplo disso é o Código de Conduta de proteção de dados - https://abes.com.br/lgpd-codigo-de-conduta-para-agentes-de-pequeno-porte/ - lançado pela ABES com o objetivo de proporcionar maior segurança jurídica aos seus associados.

Pelo exposto, reiteramos nossa disposição em contribuir para o fortalecimento e a evolução contínua da proteção de dados no Brasil, colaborando ativamente para consolidar um ambiente jurídico e tecnológico mais seguro e inovador.

Cordialmente,

THOMAZ LOPES CORTE REAL:27969427839

Assinado de forma digital por THOMAZ LOPES CORTE REAL:27969427839
Dados: 2024.12.02 12:49:28 -03'00'

ABES – ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS DE SOFTWARE
Thomaz Côrte Real
Consultor Jurídico

abesrelacionamento@abes.org.br | www.abes.org.br
Av. Ibirapuera - 2907 - 8º Andar - Cj 811 - Moema
São Paulo - SP - CEP: 04029 - 200
Telefone: + 55 11 2161 - 2833

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANEXO VII – CONTRIBUIÇÕES: ASSOCIAÇÃO BRASILEIRA DE MOBILIDADE E TECNOLOGIA (AMOBITEC)

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

AMOBITEC
Associação Brasileira de Mobilidade e Tecnologia

OF/AMOBITEC N. 94/2024

São Paulo, 10 de dezembro de 2024.

Ref.: Grupo de Trabalho nº 5 do Conselho Nacional de Proteção de Dados - Formulação da Política Nacional de Proteção de Dados

Excelentíssimo Rony Vainzof,

A **Associação Brasileira de Mobilidade e Tecnologia ("AMOBITEC")**, entidade representante das empresas que prestam serviços tecnológicos relacionados à mobilidade de pessoas ou bens, como aplicativos de delivery e intermediação de viagens de transporte individual privado de mobilidade urbana, vem, respeitosamente, apresentar **contribuições no âmbito do Grupo de Trabalho nº 5 do Conselho Nacional de Proteção de Dados, com o objetivo de subsidiar as discussões e colaborar para a formulação da Política Nacional de Proteção de Dados.**

Aproveitamos o ensejo para renovar nossos protestos da mais alta estima e desde já agradecemos a Vossa consideração.

André Alencar Porto

Diretor-Executivo

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

AMOBITEC
Associação Brasileira de Mobilidade e Tecnologia

I. CONSIDERAÇÕES INICIAIS SOBRE A PROPOSTA

Contribuições ao Grupo de Trabalho nº 5 do Conselho Nacional de Proteção de Dados (CNPD): A Importância da Proteção de Dados Pessoais no Desenvolvimento Econômico

A AMOBITEC foi convidada a apresentar contribuições no âmbito do Grupo de Trabalho nº 5 do Conselho Nacional de Proteção de Dados, que discute a importância da proteção de dados pessoais no contexto do desenvolvimento econômico, com o objetivo de subsidiar as discussões e contribuir para a formulação da Política Nacional de Proteção de Dados.

Nesta oportunidade, a AMOBITEC concentra suas contribuições em dois temas principais, amplamente debatidos tanto na recente Tomada de Subsídios promovida pela ANPD quanto nas discussões do Projeto de Lei nº 2338/2023 sobre inteligência artificial. O primeiro tema aborda a necessidade de supervisão ou revisão humana em decisões automatizadas, enquanto o segundo se refere à automatização de decisões que resultam no bloqueio ou desativação de motoristas e entregadores parceiros cadastrados em plataformas digitais, abrangendo serviços de intermediação de transporte individual privado de passageiros, delivery e outros modelos de negócio.

A Amobitec destaca a importância de abordagens regulatórias equilibradas sobre esses temas, garantindo a proteção dos direitos dos titulares em relação ao tratamento de dados pessoais, sem comprometer o potencial das tecnologias de inteligência artificial. É essencial considerar o impacto dessas tecnologias no desenvolvimento econômico digital e na promoção da inovação tecnológica, assegurando que as regulamentações não limitem avanços cruciais para a economia digital.

II. IMPORTÂNCIA DAS DECISÕES AUTOMATIZADAS

As decisões automatizadas são essenciais para o desenvolvimento econômico do trabalho em plataformas, pois otimizam a conexão entre oferta e demanda, garantindo maior eficiência operacional. A automação facilita a escalabilidade dos serviços, permitindo que as plataformas operem em múltiplos mercados simultaneamente, atendendo a um número crescente de usuários e estabelecimentos sem comprometer a qualidade do serviço. Essa eficiência cria novas oportunidades de geração de renda, tornando o trabalho em plataformas uma alternativa viável e flexível para milhões de pessoas.

Além disso, a automação e a inteligência artificial são peças-chave na criação de um ambiente mais seguro e confiável para estabelecimentos, motoristas e entregadores parceiros, e usuários.

Sistemas automatizados podem identificar comportamentos de risco, prevenir fraudes e promover a aplicação consistente de políticas, assegurando que as interações dentro da plataforma sejam justas e transparentes. Esses sistemas também permitem ajustes contínuos com base em dados em tempo real, possibilitando respostas rápidas a variações na demanda ou incidentes específicos. Tais mecanismos tornam o trabalho das plataformas mais acessível e contribuem para fortalecer a economia, ao fomentar um mercado de trabalho dinâmico, inovador e adaptado às necessidades da era digital.

No caso das plataformas digitais de mobilidade, as decisões automatizadas desempenham um duplo papel crucial:

1. **Promover o equilíbrio dinâmico entre oferta e demanda:** Utilizando múltiplas variáveis de mercado, essas decisões beneficiam todos os atores que utilizam os serviços de tecnologia das plataformas.
2. **Garantir a segurança da plataforma e de seus usuários:** Investindo em sistemas de prevenção de fraudes e proteção da integridade da plataforma, bem como na segurança dos usuários e motoristas e entregadores parceiros. Esses esforços refletem o compromisso das plataformas em oferecer um ambiente confiável e funcional.

Nesse contexto, a obrigatoriedade de revisão humana para todas as decisões automatizadas, bem como restrições indiscriminadas aos bloqueios e às desativações de contas de motoristas e entregadores parceiros, devem ser avaliadas com base no princípio da razoabilidade. É fundamental evitar que tais exigências inibam os benefícios econômicos e sociais proporcionados por essas tecnologias inovadoras. Um equilíbrio regulatório é essencial para que as plataformas continuem a oferecer soluções eficientes, seguras e economicamente vantajosas para a sociedade.

III. NECESSIDADE DE HUMANA PARA DECISÕES AUTOMATIZADAS

I) Os direitos já oferecidos ao titular pela LGPD

O artigo 20 da LGPD assegura o direito à revisão de decisões tomadas unicamente por sistemas automatizados que afetem os interesses dos titulares de dados, em atendimento aos princípios da necessidade, da transparência e da não discriminação[1]. Portanto, não há previsão de revisão humana para todas as

[1] Artigo 6º, incisos II, VI e IX.

decisões, por entendimento do legislador de que tal previsão seria inexequível, considerando a ampla dimensão da utilização de tais ferramentas e a impossibilidade da obrigação onerosa de ter uma revisão humana para cada uma delas.

De nossa parte, entendemos que a positivação do direito à explicação na LGPD demanda do controlador que seja sim capaz de fornecer informações compreensíveis para o titular, por meio das quais o titular possa contestar a decisão automatizada referida no caput do artigo 20 e exercer outros de seus direitos.

Além disso, o direito à explicação permite ao titular entender se a decisão automatizada que afeta os seus interesses ofende ou não o princípio da não discriminação. Essa interpretação é suportada tanto pela exigência de que o tratamento de dados deve ser legítimo, explícito, informado e transparente para o titular, como pela possibilidade de auditoria do controlador por parte da ANPD, com o fim específico de verificar se o tratamento automatizado de dados pessoais tem elementos discriminatórios. A realização de auditoria se torna possível sempre que o controlador alegar a proteção de seus segredos de negócio como fundamento para não fornecimento das informações solicitadas pelo titular no exercício de seu direito à explicação.

Como resposta ao pedido de explicação por parte do titular, deve o controlador informar a lógica envolvida na tomada da decisão, o significado e as consequências previstas do tratamento automatizado para o titular dos dados pessoais. Não é dever do controlador, todavia, revelar precisamente os procedimentos matemáticos ou estatísticos que orientam o algoritmo utilizado no tratamento automatizado de dados pessoais, o que se traduz na ressalva da LGPD e de outras legislações aplicáveis de respeito aos segredos de negócio do controlador. Disso decorre que não é a informação sobre a lógica geral do sistema informático do controlador que é requerida pelo direito à explicação, mas sim a informação de como o sistema tratou especificamente os dados do titular na situação por ele impugnada.

Diante desse desafio, é importante compreender sob quais condições pode ser necessária a revisão humana de decisões automatizadas com vistas à adequada garantia de direitos dos titulares. Qualquer regulação sobre decisões automatizadas, uso de algoritmos e inteligência artificial que tratem dados pessoais deve ser proporcional ao risco. Decisões automatizadas em empresas como as associadas da Amobitec geralmente apresentam baixo risco e são utilizadas para operar a plataforma em escala.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

AMOBITEC
Associação Brasileira de Mobilidade e Tecnologia

As empresas associadas da Amobitec operam no mundo físico. Padrões de tráfego, viagens e uso podem ser muito bem previstos com baixos riscos para os indivíduos. Quando usuários pedem uma pizza ou veem o tempo estimado de chegada (ETA) do entregador parceiro no aplicativo, eles entendem intuitivamente que a tecnologia que trata dados de forma totalmente automatizada está envolvida.

II) *especificação dos casos em que cabe a revisão humana para além do art 20 da LGPD*

É importante que o controlador tome as medidas necessárias para reduzir a probabilidade de erros e de consequências de efeitos discriminatórios de decisões automatizadas. Nesse sentido, trata-se do direito à revisão da decisão para que o titular possa contestar a decisão inicialmente tomada e obter nova decisão por parte do controlador.

O direito à revisão humana de decisões automatizadas - previsto na legislação europeia, mas não recepcionado pela LGPD - caso venha a ser implementado no ordenamento jurídico brasileiro, deve se focar em decisões automatizadas que tomam, ou são um fator substancial na tomada de, uma decisão que impacte significativamente direitos e liberdades fundamentais. Assim, o direito à revisão humana **não** se destina a decisões, ainda que automatizadas, que:

- Executem uma tarefa procedimental específica;
- Sirvam à detecção de padrões de tomada de decisão ou desvios de padrões anteriores de tomada de decisão, sem a intenção de substituir ou influenciar uma avaliação humana previamente concluída;
- Sejam utilizadas em tecnologias tais como:
    - Prevenção à fraude e à segurança do titular;
    - Segurança da informação, como anti malware, antivírus, firewall, filtros contra spam e robocalls;
    - Calculadoras, planilhas e bancos de dados;
    - Registro de domínios, carregamento de sites, gestão de redes, web caching, hospedagem de sites ou qualquer tecnologia similar;
    - Armazenamento de dados;
    - Matching ou pairing;
    - Correção ortográfica;
    - Comunicação com consumidores em linguagem natural com o objetivo de fornecer informações, fazer indicações ou recomendações, e responder a perguntas (chatbot), desde que sujeita a uma política de uso aceitável que proíba a geração de conteúdo discriminatório ou prejudicial.

De outra forma, uma decisão que impacte significativamente direitos e liberdades fundamentais refere-se a uma decisão que tenha um efeito legal ou material na vida de um indivíduo. Por exemplo, a União Europeia considera[2] os seguintes casos como sistemas de IA de alto risco, em que decisões automatizadas que envolvam o tratamento de dados pessoais podem ter impacto significativo sobre titulares: infraestruturas críticas, que poderiam colocar em risco a vida e a saúde dos cidadãos; educação ou treinamento vocacional, que podem determinar o acesso à educação e moldar o curso profissional de uma pessoa (por exemplo, pontuação em exames); componentes de segurança de produtos (como aplicações de IA em cirurgias assistidas por robôs); serviços essenciais privados e públicos (como pontuação de crédito que negue aos cidadãos a oportunidade de obter um empréstimo); gestão de migração, asilo e controle de fronteiras (como verificação de autenticidade de documentos de viagem); ou administração da justiça e processos democráticos. Aplicações de sistemas de IA, algoritmos e decisões automatizadas que não possuem um nível elevado de impacto não deveriam ensejar o direito à revisão humana.

Essa posição foi adotada pela mais recente versão do PL nº 2338/2023, de relatoria do Senador Eduardo Gomes (PL-TO) e aprovada na comissão do Senado criada para analisar propostas de regulamentação da inteligência artificial, que, em seu art. 6º, inciso III, limita o direito à revisão humana de decisões a pessoa ou grupo afetado por sistemas de IA de alto risco.

IV. DECISÕES AUTOMATIZADAS EM RELAÇÃO ÀS DESATIVAÇÕES

Para todas as associadas da Amobitec, não é do interesse das plataformas promover a desinformação de motoristas e entregadores parceiros, tampouco proceder com a suspensão ou bloqueio de motoristas, entregadores, usuários ou exclusão de estabelecimentos sem a devida necessidade ou justificativa. No entanto, as plataformas precisam zelar pela integridade de seus sistemas e pela segurança de todas as partes que utilizam seus serviços.

Por exemplo, diariamente há inúmeras tentativas de fraude nas plataformas, como a utilização de versões adulteradas do aplicativo, softwares que simulam posições de GPS, entre outros. Nesse contexto, as plataformas estão constantemente aprimorando seus mecanismos de proteção para enfrentar essas tentativas, que se renovam continuamente. Exemplos concretos incluem:

- Uso de meios inapropriados, diretos ou indiretos, para obter vantagens indevidas, como ganhos maiores, promoções, códigos promocionais, taxas

[2] https://futurium.ec.europa.eu/sites/default/files/2021-10/Kop_EU%20Artificial%20Intelligence%20Act%20-%20The%20European%20Approach%20to%20AI_21092021_0.pdf

de cancelamento, valores de viagens, avaliações elevadas ou obtenção do produto sem intenção de pagá-lo.
- Aceitação de solicitações de viagem ou entrega sem a intenção de concluí-las, com o objetivo de provocar o cancelamento pelos usuários.
- Início de uma viagem sem estar no ponto de embarque ou não encerrá-la no momento e local corretos.
- Abuso do serviço de suporte das plataformas, realizando solicitações falsas para obter vantagens indevidas.
- Manipulação dos sistemas das plataformas para alterar o seu funcionamento correto, entre outros.

Esses exemplos evidenciam casos em que a inteligência artificial (IA) possui uma capacidade de análise infinitamente superior para identificar fraudes, sendo a desativação ou bloqueio da conta identificada a única medida eficaz para prevenir tais ações. Restringir essas ferramentas enfraqueceria a integridade dos sistemas das plataformas e comprometeria a segurança dos usuários que utilizam seus serviços, considerando que milhares de casos acontecem todos os dias.

Não obstante, a Amobitec também reconhece que tais decisões têm um efeito considerável sobre a vida dos titulares afetados. Por essa razão, as associadas da Amobitec oferecem revisão humana para todos os casos de desativação, garantindo que nenhuma decisão automatizada seja definitiva sem possibilidade de contestação. Muitas plataformas associadas publicam, em suas páginas, as razões que podem levar à desativação, bem como os processos e orientações para solicitação de revisão, seja a decisão automatizada ou não[3]. Contudo, a única maneira de verificar motoristas ou entregadores parceiros com segurança, monitorar incidentes e desativar os motoristas ou entregadores parceiros ou usuários que representem um risco à segurança, em larga escala, é por meio do uso da IA.

Nesse sentido, é essencial que essa ferramenta, imprescindível para o desenvolvimento econômico, seja preservada, acompanhada pela possibilidade de revisão humana sempre que solicitada.

V. CONCLUSÃO

A inteligência artificial para a tomada de decisões tornou-se uma ferramenta fundamental para as plataformas associadas da Amobitec. Por essa

[3] Páginas das plataformas sobre desativações podem ser acessadas: no caso da Uber, há uma página sobre as razões das desativações, disponíveis em: https://www.uber.com/br/pt-br/drive/safety/deactivations/ e sobre como solicitar o processo de revisã, disponível em: https://www.uber.com/pt/pt-pt/drive/driver-app/deactivation-review/ .

razão, muitas dessas empresas têm desenvolvido políticas internas de governança para tratar, de maneira equilibrada, os temas abordados nesta contribuição, garantindo os direitos legais dos titulares e a segurança das plataformas e seus usuários[4][5].

Dessa forma, a Amobitec solicita cautela na análise desses tópicos, de modo a não frear o desenvolvimento econômico, especialmente considerando que existem alternativas razoáveis e equilibradas que asseguram os direitos legais e fundamentais dos titulares e promovam um desenvolvimento econômico sustentável.

Agradecemos a atenção e permanecemos à disposição para quaisquer esclarecimentos necessários.

Com os elevados votos de estima e consideração,

André Alencar Porto | Diretor Executivo – AMOBITEC

diretoriaexecutiva@amobitec.org | (61) 98105-0055

[4] A Uber, por exemplo, disponibiliza página sobre a sua governança em relação a inteligência artificial, disponível em: https://www.uber.com/us/en/about/responsible-ai/?nocache=true

[5] O iFood também disponibiliza uma página com informações sobre a utilização da inteligência artificial com os respectivos princípios que regem esse uso, disponível em: https://privacidade.ifood.com.br/inteligencia-artificial/

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANEXO VIII – CONTRIBUIÇÕES: ASSOCIAÇÃO DAS EMPRESAS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO E DE TECNOLOGIAS DIGITAIS (BRASSCOM)

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

Brasscom

CARTA DE PRINCÍPIOS SOBRE POLÍTICAS DE ECONOMIA DE DADOS - GESTÃO, COMPARTILHAMENTO E ESPAÇOS DE DADOS

A transformação digital que poderá garantir o desenvolvimento econômico e social do País requer, para seu sucesso, um conjunto massivo de dados, assim como um sistema que permita o uso e reuso destes. Nesse sentido, para que o Brasil possa aproveitar os benefícios desta transformação, inclusive da IA, é fundamental que esforços amplos e coordenados sejam realizados para viabilizar o compartilhamento de dados.

À medida que o Brasil busca solidificar sua posição na economia digital global, a criação de uma Política Nacional para Economia de Dados tem o potencial de remodelar indústrias, impulsionar a inovação e desbloquear novas oportunidades em todos os setores. Assim, é estratégica a priorização do fomento à inovação e à infraestrutura digital, principais gargalos para o desenvolvimento da economia de dados nacional. Além disso, é imperioso o foco na formação e capacitação para profissionais do setor privado e da administração pública, a ser feito a partir do diálogo em uma construção conjunta.

Nesse contexto, os espaços de dados são ecossistemas integrados e complexos onde, os agentes interagem de acordo com políticas e regras específicas compartilhadas. Isto facilita as transações de dados mais complexas, tais como a especificação de limites sobre como e para que fins os dados podem ser reutilizados.

Segue abaixo os princípios em relação à gestão, compartilhamento e espaços de dados:

1. **Fomento à inovação e livre iniciativa:** Garantir que os espaços de dados sejam ambientes voltados à inovação e impulsionadores do desenvolvimento econômico e da livre iniciativa, em harmonia com a Lei da Liberdade Econômica (Lei 13.874/2019), buscando melhor posicionar o Brasil nas cadeias globais de valor.

2. **Dados Abertos:** A economia de dados demanda uma ampliação e consolidação da política de dados abertos custodiados pelo Estado a partir da proatividade da Administração Pública em compartilhar dados com todas as partes interessadas, de modo a viabilizar a utilização e reutilização de dados para fins inovadores. Os dados compartilhados pelo Poder Público precisam ser relevantes, facilmente acessíveis, utilizáveis e reutilizáveis, de modo que a acessibilidade aprimorada possa permitir maior colaboração entre governo, setor privado e sociedade.

3. **Adesão voluntária:** Os espaços de dados são ambientes voluntários, em que pessoas, naturais ou jurídicas, podem determinar sua participação. Os agentes podem determinar também quais dados compartilhar, com quem e definir as regras para a sua reutilização por terceiro.

4. **Boa-fé na (re)utilização:** Os dados compartilhados nos espaços de dados devem ser utilizados e reutilizados com observância ao princípio da boa-fé e o respeito às regras definidas pelo compartilhador do dado, assim como o contexto original da finalidade da coleta.

5. **Descentralização:** Os espaços de dados referem-se a uma infraestrutura aberta e descentralizada para a troca de dados sem intermediários, onde padrões e diretrizes de alto nível são estabelecidos entre os próprios agentes.

6. **Interoperabilidade:** Os espaços de dados devem facilitar formatos que permitam a interação dos dados de maneira eficaz e eficiente.

7. **Padronização:** Os dados devem ser disponibilizados em um formato sobre o qual nenhuma parte tenha controle exclusivo, utilizando padrões simples e abertos para facilitar o fluxo, reduzir a complexidade dos sistemas e sua adoção por todas as partes interessadas.

8. **Transparência:** Espaços de dados devem buscar infraestrutura técnica e modelos de governança que possibilitem os agentes reunir, acessar, tratar, utilizar e compartilhar dados de forma confiável e transparente.

9. **Respeito ao segredo comercial e industrial:** Os espaços de dados devem ser estruturados sempre de maneira a respeitar limitações existentes nos usos e compartilhamento de dados, além de respeitar o segredo comercial e industrial.

10. **Privacidade e Proteção de Dados:** Os dados compartilhados nos espaços de dados, quando envolverem dados pessoais, devem ser tratados em consonância com a Lei Geral de Proteção de Dados (LGPD).

11. **Sinergia entre Espaço de Dados e Dados Abertos:** Dados abertos e espaços de dados agregam valor um ao outro. O seu cruzamento tem o potencial de criar casos de reutilização inovadores que não seriam possíveis sem esta interação, mas não podem ser confundidos em sua natureza ou função.

12. **Fomento a Políticas Públicas para Negócios Baseados em Dados:** Estimular mecanismos que possibilitem negócios baseados em dados, dentre eles criação de espaços de dados voluntários.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

Brasscom

CARTA BRASSCOM DE PRINCÍPIOS PARA DADOS ABERTOS DE GOVERNO

São Paulo, 9 de fevereiro de 2021

O conceito de dados abertos é uma filosofia que promove a transparência, a responsabilidade e a criação de valor a partir da disponibilização de conjuntos de dados do governo para todos. Os órgãos públicos produzem e coletam uma ampla gama de diferentes tipos de dados para realizar suas tarefas. A extraordinária quantidade e centralidade dos dados coletados pelos governos tornam esses dados particularmente significativos como um recurso para aumentar a transparência pública. Em face as fenomenologias da Era Digital, a filosofia de dados perfila-se, cada vez mais, em uma poderosa ferramenta para concepção e implementação de políticas públicas de qualidade que supram as demandas da sociedade e da economia intensiva em dados.

Segundo a **OCDE**, a política de dados abertos, já adotada em diversos países, tem como objetivo a criação de valor econômico para o setor privado e para a sociedade como um todo, na busca de soluções mais ágeis e efetivas para os problemas públicos da sociedade. Afinal, ao incentivar o uso, a reutilização e a distribuição de conjuntos dados de diversas naturezas, os governos acabam por promover também a criação de negócios e serviços inovadores centrados no cidadão.

Naturalmente, é necessário que as iniciativas de dados abertos de governo sejam implementadas para promover o uso eficaz de dados governamentais por parte da sociedade e atores econômicos. Os dados precisam ser relevantes, facilmente acessíveis, utilizáveis e reutilizáveis por todos. Dados abertos podem incluir dados referentes à mobilidade urbana, condições climáticas, estatísticas, entre outros. A acessibilidade aprimorada de dados pode permitir maior colaboração dentro dos governos, bem como entre agências governamentais e a sociedade em geral, incluindo o setor privado, organizações da sociedade civil e cidadãos.

Com base no exposto, a **Brasscom** apresenta, a seguir, uma proposta princípios norteadores para dados abertos de governo, com o intuito de promover a harmonização de práticas de coleta, agregação e disponibilização de dados relevantes, com o intuito de facilitar a sua utilização pelas partes interessadas, por meio do uso de tecnologias digitais, em particular, as baseadas em inteligência artificial, tais como, *machine learning*, potencializam retornos de investimento a disponibilização de serviços públicos eficientes e de qualidade, bem como, o avanço de ofertas de serviços e utilidades por parte dos agentes econômicos.

PRINCÍPIOS DE DADOS ABERTOS

1. **Dados Abertos por padrão.** Todos os dados públicos, ou seja, aqueles que não estão sujeitos a limitações legislativas ou normativas válidas de privacidade, segurança ou controle de acesso, devem ser disponibilizados para o mais amplo público, permitindo o seu uso para os mais variados propósitos.

2. **Boa-fé na utilização**. Os dados abertos disponibilizados devem ser utilizados com observância ao princípio da boa-fé.

3. **Livre de licenças**. Os dados disponibilizados de forma aberta não devem estar sujeitos a restrições de uso decorrentes de direitos de propriedade intelectual, tais como, direitos autorais, marcas, patentes ou segredo industrial.

4. **Legíveis por máquina**. Todos os dados públicos, que sejam passiveis de abertura, devem ser disponibilizados em formatos abertos e legíveis por máquina, a fim de permitir a análise e a utilização de forma facilitada.

5. **Disponibilização a partir da coleta primária**. Os dados devem ser disponibilizados na forma coletada na fonte, com a mais fina granularidade possível, e não de forma agregada, prezando, sempre, pelo uso de mecanismos que removam a identificabilidade do dado, em observância às leis vigentes.

6. **Disponibilização tempestiva**: Os dados devem ser disponibilizados o mais rápido possível para preservar a sua relevância e utilidade.

7. **Interoperabilidade**. Dados públicos referentes ao mesmo assunto devem ser publicados nos mesmos formatos padrão e com as mesmas definições, viabilizando a combinação de diferentes bases de dados, buscando sempre maior interoperabilidade.

8. **Acesso Universal**. Os dados devem estar disponíveis a todos, ainda que seja necessária identificação ou registro, especialmente para fins de atendimento.

9. **Padronização**. Os dados devem ser disponibilizados em um formato sobre o qual nenhuma parte tenha controle exclusivo, utilizando padrões simples e abertos para facilitar o fluxo de dados, reduzir a complexidade dos sistemas e facilitar a sua adoção por todas as partes interessadas.

10. **Documentação**. A disponibilização de documentação contendo mais informações sobre o formato e o significado dos dados é uma forma de potencializar a sua utilidade.

11. **Governo Aberto**. As informações sobre as atividades de governo deverão ser abertas e compreensíveis, de forma a aumentar a transparência, a prestação de contas e a participação cidadã.

12. **Governança de dados abertos**. Se faz mister a constituição de um Comitê Multissetorial com a participação do governo, sociedade civil, academia e setor produtivo para a estabelecer as orientações sobre a melhor política pública para a adoção de dados abertos. A atuação deste órgão deve ser focada em:

    12.1. Apoiar o desenvolvimento de dados abertos como premissa para a transparência na Administração Pública;

    12.2. Auxiliar no cumprimento da legislação, políticas e normas relevantes em vigor; na implementação de iniciativas de dados abertos no setor público; e

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

Brasscom

12.3. Fornecer orientação e compartilhar experiências sobre a implementação de dados abertos na Administração Pública Direta e Indireta, incentivando, assim, o compartilhamento de dados governamentais, melhorando a qualidade e a transparência da prestação de serviços e promovendo o crescimento econômico do país por meio de inovações.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANEXO IX – CONTRIBUIÇÕES: ASSOCIAÇÃO NACIONAL DOS BUREAUS DE CRÉDITO (ANBC)

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANBC
ASSOCIAÇÃO NACIONAL DOS BUREAUS DE CRÉDITO

São Paulo, 02 de dezembro de 2024

Ao
Sr. Rony Vainzof – Conselheiro Titular e Coordenador do GT 5 do CNPD
Email: rony@vllaw.com.br

1

Prezado Sr.

Pelo presente, na qualidade de representantes da Associação Nacional dos Bureaus de Crédito – ANBC, entidade que reúne os bureaus atuantes no território brasileiro, com o objetivo de representar o setor de banco de dados de crédito no país, honrados com a possibilidade de contribuir com o Grupo de Trabalho estabelecido pela Portaria CNPD nº 05/24, vimos apresentar contribuições em relação às questões que nos foram encaminhadas via ofício, conforme abaixo:

1- **Casos práticos e dados estatísticos que demonstrem a importância do uso e da proteção de dados pessoais para o desenvolvimento econômico, tecnológico e a inovação.**

Um caso prático e de grande relevância para o setor dos bureaus de crédito é a implantação do Cadastro Positivo, que trouxe um aumento de 78% na nota de crédito dos consumidores. Além disso, aumentou a visibilidade de 21 milhões de pessoas físicas e jurídicas que, por não terem muitas vezes uma conta junto a instituições financeiras – os chamados desbancarizados – eram totalmente invisíveis ao mercado de crédito.

De outro lado, dos consumidores que pediram para sair do programa, 83% já solicitaram seu retorno, por perceberem os reflexos positivos em relação ao acesso ao crédito. Com efeito, o Cadastro Positivo, em cinco anos, aumentou em dezoito vezes a chance de acesso ao crédito de qualidade, em todas as regiões do país. Desse modo, trouxe democratização do crédito e bem-estar social.

Importante salientar que a LGPD deixa clara a possibilidade de uso desses dados pelos GBDs, ao dispor, em seu artigo art. 7º, inciso X, não ser obrigatório o consentimento do titular dos dados "para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente".

Assim, os GBDs, ao receberam os dados, realizam a análise de risco de crédito do cadastrado, ao passo que os consulentes desses dados podem usar essas informações para subsidiar a concessão ou extensão de crédito e a realização de venda a prazo ou outras transações comerciais que impliquem risco financeiro ao consulente.

Ademais, o CP se consolidou como um direito do consumidor, justamente por permitir que tal consumidor tenha acesso facilitado a uma proposta de crédito mais justa e adaptada à sua realidade, uma vez que o uso dos dados para a formação do cadastro permitiu não só que as empresas possam conhecer mais clientes em potencial, mas conhecê-los melhor, ao reduzir a assimetria de informações.

Seguem alguns dados estatísticos sobre registros no Cadastro Positivo nos diversos setores recrutados pelo cadastro, em busca de incluir informações de pessoas que não se relacionam com bancos:

a) Instituições financeiras: 147mi;
b) Telecom: 97mi;
c) Energia: 75mi;
d) Saneamento: 55mi;
e) Gás encanado: 4mi.

Em relação às empresas no CP, temos os seguintes percentuais: (i) MEI: 16,56%; (ii) Micro: 49,97%; (iii) Pequena: 68,93%; (iv) Média: 69,15%; (v) Grande: 93,58%.

Na mesma linha, citamos o SCR (Sistema de Informações de Crédito) do Banco Central, com 1230 fontes e 144 milhões de registros, sendo 4,85 mi de pessoas físicas e 1,1 mi de pessoas jurídicas.

2- Como a LGPD e outras normas aplicáveis, nacionais e internacionais, servem como bússola para que os dados pessoais possam ser utilizados para o desenvolvimento econômico, tecnológico e a inovação, de forma ética, segura e responsável?

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANBC
ASSOCIAÇÃO NACIONAL DOS BUREAUS DE CRÉDITO

A LGPD, ao prever a forma de coleta, tratamento e armazenamento dos dados pessoais e sensíveis, bem como ao regulamentar as operações e transferências de dados e as sanções aplicáveis aos infratores, atrai mais investimentos ao país, pois demonstra o alinhamento do Brasil em relação às leis internacionais.

De fato, a LGPD trouxe a oportunidade de aperfeiçoamento das políticas de governança de dados, com adoção de regras de boas práticas e incorporação de medidas técnicas e administrativas que mitiguem os riscos e aumentem a confiança dos titulares dos dados na organização. Por consequência, aumenta o controle do cidadão quanto aos seus dados pessoais, a transparência e a segurança jurídica, além de elevar o nível de maturidade, ética e competitividade de nossas organizações.

Igualmente, a articulação da ANPD com outras entidades e órgãos públicos auxiliam o crescimento da segurança das informações e o estabelecimento de outras normas e diretrizes, com maior eficiência. Aliás, a ANPD já publicou diversos documentos e guias orientativos sobre a LGPD.

Da mesma forma, a função consultiva do CNPD será importante na conformação do ambiente regulatório de proteção de dados pessoais, na medida em que viabiliza a participação dos diferentes segmentos da sociedade.

Na mesma linha, a União Europeia mantêm em vigor desde 2018 seu regulamento, o *General Data Protection Regulation*, que impulsionou o Brasil na elaboração da LGPD.

Desse modo, a LGPD coloca o Brasil em conectividade de livre acesso a informações, afora a multidisciplinaridade de conhecimentos que se relacionam pela governança, tratamento de dados e pela segurança nas informações.

O meio digital disponibiliza uma série de ferramentas que visam assegurar esse processo de coleta de dados em face das normativas ensejadas pela LGPB, assegurando, por meio de procedimentos internos e políticas de privacidade, toda e qualquer atividade que demandem o uso de dados.

3- Quais práticas poderiam ser implementadas para melhorar a proteção de dados e segurança jurídica no tratamento de dados pessoais para o desenvolvimento econômico, tecnológico e a inovação?

Considerando o cenário atual, em que a contribuição dos dados cresce de maneira exponencial e com amplos benefícios à sociedade, a ANBC acredita que práticas relacionadas à

transparência, acesso e ao tratamento das informações são fundamentais para o desenvolvimento econômico, tecnológico e inovação.

Dentre as inúmeras já usualmente utilizadas, consideramos que a implementação de políticas de privacidade claras e transparentes auxiliam diretamente a melhor gestão pelo titular de dados em relação aos seus dados. No documento em questão, imprescindível que informações como quais são os dados coletados e para quais finalidades são tratados, tal qual prevê o artigo 9º da Lei Geral de Proteção de Dados.

Em relação ao tratamento de dados em si, vale indicar a criptografia como ferramenta eficaz para proteger as informações durante a transmissão e armazenamento, auxiliando inclusive no controle de acesso às informações, reduzindo o risco de eventual uso ou compartilhamento indevidos.

Já quando avaliamos as práticas relacionadas às pessoas, entendemos como fundamental o treinamento e conscientização dos colaboradores e/ou parceiros dos agentes de tratamentos de dados. A capacitação contínua sobre as melhores práticas de segurança, privacidade e situações de risco auxiliam não só os agentes de tratamento a cumprirem a legislação e terem a política da empresa disseminada, como ajuda o próprio titular de dados garantindo que todos aqueles envolvidos tenham consciência dos seus papeis e responsabilidades.

Por final, destacamos o controle de acesso às informações. A implementação de controles como: fatores de autenticação e/ou políticas envolvendo a criação de senhas consideradas fortes, é essencial para garantir que apenas os titulares de dados respectivos tenham acesso às informações, principalmente aquelas consideradas sensíveis.

Sem mais, subscrevemo-nos.

Cordialmente DocuSigned by: Elias Sfeir 8A58DA16B46D4AF...

ANBC – Associação Nacional dos Bureaus de Crédito
Elias Sfeir -Diretor Presidente

DS LHVPP

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANEXO X – CONTRIBUIÇÕES: CONEXIS BRASIL DIGITAL

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

conexis brasil.digital

Brasília/DF, 28 de novembro de 2024

Assunto: Contribuições na temática de dados pessoais para o desenvolvimento econômico, tecnológico e a inovação, para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade.

Órgão: CNPD – Conselho Nacional de Proteção de Dados.

Área: GT5

Contribuições Conexis Brasil Digital ao Conselho Nacional de Proteção de Dados para a elaboração da Política Nacional de Proteção de Dados Pessoais

1. Casos práticos e dados estatísticos que demonstrem a importância do uso e da proteção de dados pessoais para o desenvolvimento econômico, tecnológico e a inovação;

A digitalização, cada vez mais presente na vida das empresas e das pessoas, tem o potencial de revolucionar o nosso cotidiano, com soluções para importantes desafios nacionais em áreas como mobilidade urbana, eficiência energética, atendimento à saúde e produtividade industrial. Nesse sentido, as **Infraestruturas Públicas Digitais (DPIs)**, tem papel essencial para o desenvolvimento econômico, tecnológico e da inovação. O DPI é uma infraestrutura única consistente dentro do governo, que perpassa todas as entidades, e viabiliza uma integração de dados em todos os níveis do setor público, evitando-se a duplicação de informações, ou até mesmo quaisquer tipos de indisponibilidade ou conflito entre informações. Em termos práticos, como referência ao cenário brasileiro, podemos citar o Governo como **Plataforma (gov.br)**, onde as pessoas naturais têm uma identidade digital única para acessar os diversos serviços públicos perante os mais diversos órgãos do governo.

Além disso, temos o caso do **Pix**, meio de pagamento instantâneo criado pelo Banco Central, que viabiliza transferência em tempo real entre contas de bancos diferentes, conferindo segurança às transações, devido à integração de sistemas que permitem a verificação da

SCN Quadra 04 Bloco B – Centro Empresarial Varig – Sala 1101 – CEP. 70714-900 – Asa Norte – Brasília - DF
Tel: (61) 2105-7455 email: conexis@conexis.org.br www.conexis.org.br

identidade dos usuários e a autenticidade das solicitações de pagamento. Como outro exemplo, podemos destacar o uso da rede de telecomunicações em benefício público no momento da pandemia do Covid-19, em que foi disponibilizado aos órgãos públicos, de forma segura e anônima, um **mapa de calor**, permitindo medir deslocamentos. Isso permitiu aos estados e municípios identificar em quais regiões o isolamento social não estava sendo cumprido, para aplicação de ações localizadas a fim de diminuir a circulação de pessoas, auxiliando o poder público na contenção da pandemia.

Outrossim, o setor de telecomunicações enfrenta constantemente o desafio de combater diversos tipos de fraudes. O uso de dados pessoais para o desenvolvimento econômico e tecnológico, são de suma importância, a título de exemplo podemos citar as soluções baseadas em dados pessoais que visam promover a segurança dos titulares, como as de **prevenção a prática de fraudes**. Grandes empresas que fazem gestão de bases de dados pessoais, podem contribuir de forma exponencial para um mercado cada vez mais seguro, provendo soluções que não necessariamente precisem operar com o compartilhamento de dados pessoais, mas que se utilizem os dados para o desenvolvimento de modelos de negócios para o enfrentamento e combate a fraudes.

Um relatório divulgado pelo Serasa[1] revelou dados alarmantes: em 2022, foi registrada uma tentativa de fraude a cada oito segundos no Brasil, totalizando mais de 3,9 milhões de incidentes. Já em 2023[2], o número quase triplicou, com cerca de 10 milhões de tentativas identificadas, demonstrando um aumento expressivo em comparação aos anos anteriores. A instituição destacou, ainda, a importância de as empresas investirem em soluções de autenticação e mecanismos robustos de prevenção à fraude.

Entretanto, as fraudes podem ter consequências ainda mais graves quando falamos do setor de telecomunicações, pois o acesso indevido às linhas telefônicas de clientes pode ser

[1] Disponível em https://www.serasaexperian.com.br/sala-de-imprensa/estudos-e-pesquisas/brasil-encerra-2022-com-quase-39-milhoes-de-tentativas-de-fraude-de-identidade-revela-serasa-experian/ Acesso em 26/11/2024.
[2] Disponível em https://www.serasaexperian.com.br/sala-de-imprensa/prevencao-a-fraude/quase-10-milhoes-de-tentativas-de-fraude-de-identidade-foram-registradas-em-2023-mostra-serasa-experian/ Acesso em 26/11/2024

SCN Quadra 04 Bloco B – Centro Empresarial Varig – Sala 1101 – CEP. 70714-900 – Asa Norte – Brasília - DF
Tel: (61) 2105-7455 email: conexis@conexis.org.br www.conexis.org.br

explorado como ponto de partida para outros crimes, como a obtenção de contas de e-mail vinculadas, muitas vezes utilizadas para recuperação de senhas. A partir dessas contas, fraudadores podem acessar diversos serviços associados ao titular, desde simples perfis em plataformas de comércio eletrônico até contas bancárias.

Diante desse cenário, o setor de Telecom vem adotando medidas para proteger seus clientes de alterações indevidas realizadas por terceiros, que frequentemente falsificam documentos para cometer fraudes. Entre essas iniciativas, destacamos a **implementação da biometria facial em processos de venda, contratação e alteração de planos**, troca de SIM card, substituição de aparelho, transferência de titularidade e cancelamento de produtos. Essa tecnologia é reconhecida como uma das mais eficazes na prevenção de golpes e é amplamente aceita pelos consumidores, que afirmam sentir maior segurança com a biometria facial em comparação à leitura de digitais.

Essa medida também é respaldada pela ANATEL, que confirma a relevância da biometria facial como uma das principais estratégias adotadas pelo setor para combater fraudes e golpes. Além disso, tal prática atende a exigências legais às quais o setor está sujeito, conforme disposto no artigo 65-M do Regulamento de Serviços de Telecomunicações[3].

O uso de tecnologias e ferramentas de comunicação, especialmente a telefonia móvel, que alcança cerca de 97% da população brasileira, traz a oportunidade de aproveitar os dados de telecomunicações para suprir lacunas de informação sobre o risco de inadimplência. Isso é particularmente relevante para o desenvolvimento econômico e social ao facilitar o acesso ao crédito com condições mais favoráveis, promovendo inclusão econômica e social para a população de baixa renda.

Esse movimento é essencial para a economia brasileira, especialmente diante dos seguintes aspectos:

[3] Disponível em https://informacoes.anatel.gov.br/legislacao/resolucoes/2020/1495-resolucao-738 Acesso 26/11/2024

SCN Quadra 04 Bloco B – Centro Empresarial Varig – Sala 1101 – CEP. 70714-900 – Asa Norte – Brasília - DF
Tel: (61) 2105-7455 email: conexis@conexis.org.br www.conexis.org.br

- Desbancarização e informalidade: Parcela significativa da população brasileira não possui conta bancária e aproximadamente 41% atuam no mercado informal (dados do IBGE, 2019[4]). Essa realidade limita as informações disponíveis para análise de crédito, conforme destacado pelo Serasa, especialmente entre indivíduos que não participam do Cadastro Positivo.
- Endividamento e inadimplência: Dados da OCDE[5] mostram que, embora o nível de endividamento no Brasil seja baixo em comparação com outros países, o índice de inadimplência é um dos mais elevados da América Latina.

Estudos reforçam esse panorama. O Instituto Locomativa[6] estimou que, em 2021, cerca de 34 milhões de brasileiros eram desbancarizados ou pouco utilizavam suas contas bancárias. Já uma pesquisa do Instituto Dom Cabral em parceria com a BRINKS[7] apontou que 38,5% da população brasileira não tinha conta bancária naquele ano.

Nesse contexto de déficit informacional, os dados oriundos do setor de telecomunicações surgem como uma alternativa relevante para aprimorar a avaliação de risco de crédito. Isso reduz as lacunas de informação e facilita a inclusão financeira. Um relatório da Financial Inclusion Global Initiative (FIGI), intitulado "Use of Telecommunications Data for Digital Financial Inclusion[8]", reforça essa ideia:

> "A ausência de dados confiáveis sobre crédito e outras informações é um dos principais desafios para ampliar a inclusão financeira. Os dados de

[4] Disponível em https://agenciabrasil.ebc.com.br/economia/noticia/2020-11/ibge-informalidade-atinge-416-dos-trabalhadores-no-pais-em-2019 Acesso em 26/11/2024
[5] Disponível em OECD, *Facilitating Access to Finance – Discussion Paper on Credit Information Sharing*, at https://www1.oecd.org/globalrelations/45370071.pdf. Acesso em 26/11/2024
[6] Disponível em: https://valorinveste.globo.com/produtos/servicos-financeiros/noticia/2021/04/27/34-milhoes-de-brasileiros-ainda-nao-tem-acesso-a-bancos-no-pais.ghtml. Acesso em 26/11/2024
[7] Disponível em: https://br.brinks.com/-/brink-s-se-une-%C3%A0-funda%C3%A7%C3%A3o-dom-cabral-em-pesquisa-que-traz-h%C3%A1bitos-e-prefer%C3%AAncias-dos-brasileiros-em-rela%C3%A7%C3%A3o-aos-meios-de-pagamento. Acesso em 26/11/2024
[8] Disponível em: https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-DFS-2021-5-PDF-E.pdf. Último acesso em 26.11.2024.

SCN Quadra 04 Bloco B – Centro Empresarial Varig – Sala 1101 – CEP. 70714-900 – Asa Norte – Brasília - DF
Tel: (61) 2105-7455 email: conexis@conexis.org.br www.conexis.org.br

telecomunicações podem ajudar a preencher essas lacunas, conectando informações tradicionais de crédito aos dados gerados por consumidores e empreendedores".

Dessa forma, resta claro que o uso estratégico de dados do setor de telecomunicações contribui para tornar o sistema financeiro mais inclusivo e acessível, gerando benefícios amplos para indivíduos e para o mercado como um todo, dentre eles:

- Benefícios para o titular: Dados de telecomunicações permitem a criação de scores de crédito mais precisos, resultando em decisões financeiras mais justas. Isso é especialmente significativo para usuários de serviços pré-pagos excluídos do Cadastro Positivo, incluindo indivíduos em situação de vulnerabilidade e sem histórico de crédito formal.
- Impacto para a sociedade: Novas métricas e modelos de score de crédito podem permitir uma melhor alocação de recursos financeiros pelas empresas. Isso tende a reduzir os custos do crédito e, consequentemente, o preço para os consumidores finais, diminuindo o spread bancário e promovendo maior eficiência econômica.

2. Como a LGPD e outras normas aplicáveis, nacionais e internacionais, servem como bússola para que os dados pessoais possam ser utilizados para o desenvolvimento econômico, tecnológico e a inovação, de forma ética, segura e responsável?

É inquestionável o importante papel que a Internet e a conectividade têm na sociedade atual, tanto como viabilizadora de inclusão social, quanto indutora de inovação e crescimento econômico. Em todo o mundo, o uso efetivo de dados tornou-se uma parte crítica das estratégias nacionais de desenvolvimento. Dados transformadores permitem que governos e organizações tomem decisões informadas que não apenas alimentam o crescimento econômico e o desenvolvimento, mas também acendem a inovação em vários setores.

A LGPD, enquanto principal norma aplicável, traz robusto arcabouço legal para viabilizar e fomentar o desenvolvimento econômico, tecnológico e a inovação, de forma ética

segura e responsável, ao definir diretrizes específicas para o tratamento de dados pessoais, quando estabelece parâmetros para o uso de dados.

É possível extrair esse entendimento da própria lei, quando enfatiza que a proteção de dados pessoais se baseia, entre outros princípios, na privacidade, autodeterminação informativa, livre iniciativa, livre concorrência, desenvolvimento econômico e tecnológico, e inovação. Isso evidencia a preocupação em equilibrar a proteção dos dados pessoais com a sua relevância para a economia.

Além disso, as empresas que entendem e reconhecem a importância da proteção de dados pessoais e agem em favor dos titulares possuem vantagem competitiva, especialmente em um mundo movido por dados, e é possível entender o interesse global no tema quando vemos cada vez mais lei gerais de proteção de dados sendo publicadas pelo mundo.

Uma das realidades decorrentes dessa nova realidade conectada, e que ao mesmo tempo a impulsiona, é o tráfego incessante de dados transfronteiriços, permitindo que a sociedade como um todo colha os benefícios do processo de inovação. Vale ressaltar que o livre fluxo internacional de dados vem desempenhando um papel fundamental como componente de impacto socioeconômico, na medida em que abre as portas para novas empresas físicas e digitais em diferentes lugares do mundo, possibilitando a inovação e a visibilidade de seus produtos, tanto em âmbito local quanto global. Frente ao avanço tecnológico, e à economia cada vez mais baseada em dados, é de extrema relevância o capítulo de transferência internacional de dados na LGPD, bem como a recente regulamentação da ANPD sobre o tema (Resolução no. 19/2024), que representou um primeiro passo relevante ao esclarecer alguns mecanismos importantes para viabilizar o fluxo internacional de dados, garantindo segurança jurídica e a proteção dos usuários.

O acesso a cadeias de suprimento globalizadas é uma importante fonte de crescimento socioeconômico, de geração de empregos e atração de novos investimentos, em especial para economias em desenvolvimento. A interconectividade global permite que mesmo as pequenas empresas nasçam globalmente: 86% das startups baseadas em tecnologia

SCN Quadra 04 Bloco B – Centro Empresarial Varig – Sala 1101 – CEP. 70714-900 – Asa Norte – Brasília - DF
Tel: (61) 2105-7455 email: conexis@conexis.org.br www.conexis.org.br

pesquisadas pelo McKinsey Global Institute[9] relatam algum tipo de atividade transfronteiriça. Essa conectividade possibilita que pequenas empresas concorram com as maiores multinacionais. Os fluxos globais, de todos os tipos, suportam o crescimento ao aumentar a produtividade e os fluxos de dados estão ampliando esse efeito ao ampliar a participação de criar mercados mais eficientes. De acordo com o McKinsey Global Institute, ao longo de uma década, todos os tipos de fluxos que atuam em conjunto aumentaram o PIB mundial em 10,1% em relação ao que teria resultado em um mundo sem fluxos transfronteiriços. Esse valor totalizou cerca de US$ 7,8 trilhões em 2014, e os fluxos de dados representam US$ 2,8 trilhões desse impacto. Além disso, estimativas acusam que, em 2014, os fluxos de dados representaram US$ 2,8 trilhões de PIB global e a quantidade de dados fluindo através da Internet cresceu em 44 vezes entre 2005 e 2014. A conclusão do estudo apontou que os fluxos de dados transfronteiriços agora geram mais valor econômico do que os fluxos tradicionais de bens comercializados. Ambos os influxos e as saídas são importantes para o crescimento, pois expõem as economias a ideias, pesquisas, tecnologias, talentos e melhores práticas de todo o mundo.

As normas de proteção de dados exercem um papel fundamental ao estabelecer diretrizes para o uso responsável de dados pessoais, especialmente em iniciativas voltadas ao desenvolvimento econômico, à inovação tecnológica e ao progresso sustentável. No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD) representa um marco jurídico significativo para a gestão de dados pessoais. Inspirada em normas internacionais como o GDPR, a LGPD padronizou práticas de proteção de dados, servindo como base para legislações semelhantes em outros contextos.

A LGPD introduziu conceitos inovadores e consolidou direitos fundamentais aos titulares de dados, como a transparência e a autodeterminação informativa, garantindo que os indivíduos tenham maior controle sobre suas informações pessoais. Além disso, a lei impôs responsabilidades claras aos agentes de tratamento e atribuiu à Autoridade Nacional de Proteção de Dados (ANPD) a responsabilidade de supervisionar sua aplicação, promover a conscientização sobre o tema e regulamentar normas e diretrizes que assegurem a proteção de dados.

[9] McKinsey Global Institute. *Digital globalization: The new era of global flows*, March, 2016. Disponível em: https://goo.gl/FYknVg. Acesso em 28/11/2024.

SCN Quadra 04 Bloco B – Centro Empresarial Varig – Sala 1101 – CEP. 70714-900 – Asa Norte – Brasília - DF
Tel: (61) 2105-7455 email: conexis@conexis.org.br www.conexis.org.br

Os princípios da LGPD, como finalidade, necessidade, segurança, prevenção, transparência e responsabilização orientam todas as atividades de tratamento de dados, independentemente de sua finalidade específica. Esses princípios não apenas estabelecem uma base ética para as entidades que tratam dados, mas também asseguram que o uso das informações esteja alinhado aos valores de respeito à privacidade e proteção dos direitos fundamentais. Ao cumpri-los, as organizações demonstram comprometimento com uma abordagem ética e responsável no tratamento de dados.

Assim, a previsibilidade proporcionada pela LGPD, por meio de seus princípios norteadores, não apenas apoia a conformidade legal, mas também impulsiona a inovação e o crescimento econômico ao garantir segurança jurídica, permitindo o avanço sustentável do mercado e promovendo um ambiente de confiança mútua entre empresas e consumidores. A proteção de dados não representa, portanto, um freio para a inovação, porque inovar significa responder adequadamente às novas demandas e questionamentos da sociedade, que hoje quer discutir o respeito à privacidade.

3. Quais práticas poderiam ser implementadas para melhorar a proteção de dados e segurança jurídica no tratamento de dados pessoais para o desenvolvimento econômico, tecnológico e a inovação?

Dentre as práticas a serem implementadas para garantir a proteção de dados e a segurança jurídica no tratamento de dados pessoais para o desenvolvimento econômico, tecnológico e de inovação, destacamos a **importância da edição de normativos claros e robustos pela ANPD**, com base nas prioridades identificadas pela autoridade em conjunto com a sociedade, a fim de garantir um ambiente de maior segurança jurídica tanto para os agentes de tratamento quanto para os titulares, bem como a expansão da infraestrutura pública digital brasileira, como o caso da plataforma gov.br, para aprimorar a integração e a interoperabilidade de dados do governo.

Ademais, das práticas que podem aprimorar a proteção de dados, destacamos a **regulamentação de temas** como o **uso do legítimo interesse** para justificar operações de tratamento que têm como objetivo a prevenção à fraude, proteção ao crédito e treinamento de sistemas de inteligência artificial, pois a ausência de uma regulamentação específica sobre o uso da referida base legal para os propósitos indicados gera insegurança jurídica para os agentes de tratamento.

Ressaltamos, inicialmente, que o uso da base legal do legítimo interesse para tratar dados pessoais não sensíveis com a finalidade de prevenir fraudes e garantir a segurança do titular é uma questão de grande relevância, já que pode ser aplicada tanto ao uso interno, para a organização validar a identidade do titular, quanto para o uso externo, que envolve o desenvolvimento e fornecimento de soluções que auxiliam terceiros na proteção cibernética e na validação de identidades, beneficiando não apenas seus adquirentes, mas também a sociedade e os próprios titulares contra o roubo de identidade.

Outro uso relevante do legítimo interesse é na criação de soluções para análise de risco de crédito. Essas ferramentas complementam os métodos tradicionais, baseados em históricos financeiros, e são particularmente importantes para indivíduos desbancarizados, ajudando na inclusão dessas pessoas no sistema financeiro.

Frisamos que, embora a LGPD preveja a base legal de "proteção ao crédito" no art. 7º, IX, sua aplicação é limitada a operações vinculadas a dados de crédito, como registros de restrição ou adimplemento, nos moldes da Lei nº 12.414/2011. Contudo, muitas soluções inovadoras poderiam utilizar dados alternativos, como informações de telecomunicações, para avaliar o risco de crédito de pessoas sem histórico financeiro, especialmente aquelas em situação de vulnerabilidade social.

Dessa maneira, o legítimo interesse também pode ser considerado como a base legal mais adequada para justificar o uso desses dados, permitindo o desenvolvimento de

SCN Quadra 04 Bloco B – Centro Empresarial Varig – Sala 1101 – CEP. 70714-900 – Asa Norte – Brasília - DF
Tel: (61) 2105-7455 email: conexis@conexis.org.br www.conexis.org.br

soluções que tragam decisões de crédito mais justas e equitativas, beneficiando tanto os agentes econômicos quanto os titulares.

Outrossim, temos a aplicação do legítimo interesse no treinamento de sistemas de inteligência artificial (IA). Destacamos que a referida base legal é particularmente adequada para justificar o treinamento de IAao atender tanto aos interesses dos desenvolvedores, sejam comerciais ou de pesquisa, quanto aos interesses de grupos sociais mais amplos, beneficiados pelas inovações, relevância econômica e potencial transformador trazidos por esses sistemas para o desenvolvimento socioeconômico do país. Em adição, é sabido que as demais bases legais da LGPD não atendem de maneira satisfatória as necessidades do treinamento de IA reforçando, assim, a necessidade de se considerar o legítimo interesse como adequado, desde que respeitado o teste de balanceamento.

Alternativamente, sugerimos a **possibilidade de os setores econômicos se organizarem por meio de uma autorregulação regulada**, que é uma alternativa eficiente considerando a ampla agenda regulatória da ANPD. Esse modelo permite que os próprios controladores e operadores, com base no Art. 50 da LGPD, desenvolvam e implementem regras de boas práticas e de governança que assegurem a conformidade com a lei e a segurança jurídica, mesmo antes de uma regulamentação específica ser publicada pela autoridade reguladora.

A autorregulação regulada oferece flexibilidade para adaptar normas a necessidades específicas de cada setor, incentivando associações entre empresas com interesses comuns. Por exemplo, o setor financeiro e o setor de telecomunicações poderiam colaborar para criar códigos de conduta conjuntos, dado o interesse mútuo em temas como prevenção a fraudes, proteção ao crédito e segurança cibernética.

Portanto, incentivar a autorregulação regulada não apenas complementa as iniciativas da ANPD, mas também permite que os setores liderem proativamente o estabelecimento de práticas responsáveis, contribuindo para a evolução contínua da proteção de dados no Brasil.

SCN Quadra 04 Bloco B – Centro Empresarial Varig – Sala 1101 – CEP. 70714-900 – Asa Norte – Brasília - DF
Tel: (61) 2105-7455 email: conexis@conexis.org.br www.conexis.org.br

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANEXO XI – CONTRIBUIÇÕES: FEDERAÇÃO BRASILEIRA DE BANCOS (FEBRABAN)

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

OFÍCIO Nº FB-1401/2024

São Paulo, 20 de dezembro de 2024.

Ao
Conselho Nacional de Proteção de Dados (CNPD)

Aos cuidados do Grupo de Trabalho 5 GT5 DO CNPD - DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

Assunto: Envio de Contribuições ao GT 5.

Senhores,

1 A Federação Brasileira de Bancos ("FEBRABAN"), associação sem fins lucrativos e principal entidade representativa do setor bancário brasileiro, que tem o compromisso de fortalecer o sistema financeiro e suas relações com a sociedade, assim como contribuir para o desenvolvimento econômico, social e sustentável do País, e que representa instituições financeiras integrante do seu quadro de associadas ("Associadas") vem apresentar, no arquivo anexo, suas contribuições ao Grupo de Trabalho 5 ("GT5") do Conselho Nacional de Proteção de Dados ("CNPD").

2 Esperamos que os materiais possam auxiliar qualitativamente nos trabalhos do GT5.

3 Permanecemos à disposição para quaisquer esclarecimentos ou contribuições que se façam necessários.

Respeitosamente,

Luís Vicente Magni De Chiara
Diretor-executivo de Assuntos Jurídicos

Carolina Sansão Moreira Alexandrino
Diretora Adjunta de Inovação,
Tecnologia e Cyber

Av. Brigadeiro Faria Lima / 4.300, 4º andar
04538-132 / São Paulo-SP / Brasil

55 11 3244-9800
febraban.org.br

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Anexo ao envio de Contribuições ao GT 5.

Temática: dados pessoais para o desenvolvimento econômico, tecnológico e a inovação para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade ("Política").

Em atendimento à solicitação de contribuições acima mencionada, a FEBRABAN entende que a utilização de dados pessoais deve ser vista como um motor para o desenvolvimento econômico e tecnológico, mas sempre com responsabilidade, levando-se em conta:

a) **Inovação Responsável:** A inovação tecnológica deve ser desenvolvida com base na ética e na conformidade com a Lei Geral de Proteção de dados (LGPD) e seus princípios. A utilização de dados pessoais para a criação de novos produtos e serviços deve considerar o adequado tratamento de dados do titular, o respeito aos direitos de privacidade e a segurança da informação. Deve haver estímulo às ferramentas que estimulam a inovação (ex. (i) *sandbox* regulatório com foco no mercado, favorecendo a inovação e o desenvolvimento tecnológico, com responsabilidade e observância dos direitos dos titulares; e (ii) ambiente de testes que utilizem dados pessoais, orientando quanto a boas práticas e medidas de segurança).

b) **Tratamento de Dados para Inovação:** Dados pessoais, quando tratados de maneira ética e legal, podem ser uma fonte poderosa para gerar *insights* que impulsionem a inovação em todos os setores, tais como serviços financeiros, saúde e educação. O agente de tratamento pode explorar o potencial de dados para criar soluções personalizadas, ao mesmo tempo que respeita as leis e os direitos dos titulares.

c) **Tecnologias de Anonimização e Pseudonimização:** Referidas tecnologias devem ser estimuladas, quando possível, no caso de dados pessoais sensíveis, reduzindo os riscos associados ao tratamento de dados pessoais.

d) **Promoção de Modelos de Negócio Sustentáveis:** A Política deve incentivar modelos de negócios que não apenas maximizem os benefícios econômicos, mas também promovam a transparência, a confiança e a responsabilidade no uso de dados pessoais.

e) **Promoção do letramento e da conscientização**: A Política deve garantir disseminação de conhecimento na sociedade acerca do uso de dados pessoais, seus benefícios, riscos e aspectos legais.

f) **Prevenção ao cibercrime e às fraudes:** A Política deve fomentar frentes que objetivem a redução de ilícitos relacionados a dados pessoais, em conexão e cooperação com políticas de segurança pública.

g) **Postura responsiva do órgão de supervisão:** Considerando tratar-se de tema ainda não totalmente compreendido e valorizado por toda a sociedade, entende-se que fundamental uma postura que busque entender, interpretar e reagir adequadamente às manifestações da sociedade.

Por fim, esclarecemos que as seguintes frentes poderiam estar abarcadas na Temática: Prevenção à fraude e segurança, Marketing, Educação, Criança e Adolescente, Saúde e questões laborais.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANEXO XII – CONTRIBUIÇÕES: IAB BRASIL – ASSOCIAÇÃO DE MÍDIA INTERATIVA

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

São Paulo, 25 de novembro de 2024
De: AMI – Associação de Mídia Interativa ("IAB Brasil" ou "IAB")
Para: Conselho Nacional de Proteção de Dados Pessoais e da Privacidade ("CNPD")
Ref.: Resposta Ofício - Contribuição ao Grupo de Trabalho 5 do CNPD

1. O IAB Brasil é uma entidade sem fins lucrativos que tem como principal missão o desenvolvimento da mídia interativa no Brasil, contando atualmente com mais de 200 associados, entre anunciantes, veículos produtores de conteúdo, empresas de tecnologia, agências e desenvolvedores, líderes em seu segmento no país.

2. De forma exemplificativa, o IAB Brasil busca desenvolver a publicidade online no Brasil através das seguintes ações: (i) incentivo às boas práticas para o planejamento, criação, compra, venda, veiculação e mensuração de mensagens comerciais; (ii) desenvolvimento do intercâmbio de experiências e conhecimentos técnicos de seus associados; (iii) promoção e divulgação de pesquisas e estudos que comprovem a eficiência da mídia interativa; e (iv) promoção da identificação de oportunidades de posicionamento da mídia interativa através de linguagem publicitária, para atrair o interesse de anunciantes e profissionais da mídia tradicional. Mais informações sobre o IAB Brasil estão disponíveis no site <https://iabbrasil.com.br/sobre-iab/>.

3. O Grupo de Trabalho 5 ("GT"), instituído conforme Portaria CNPD nº 05 de 4 de outubro de 2024, tem por objetivo levantar evidências e fornecer subsídios **acerca da importância da proteção de dados pessoais para o desenvolvimento econômico, tecnológico e a inovação, para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade (PNPD)**, conforme previsto na Lei Geral de Proteção de Dados ("LGPD") (conjuntamente considerado "Estudo").

4. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade ("CNPD"), solicitou por meio de ofício contribuições do IAB Brasil, especialmente no âmbito do Marketing e Publicidade ("Ofício"), acerca dos seguintes tópicos, os quais serão posterior e individualmente comentados pelo IAB:

i) Casos práticos e dados estatísticos que demonstrem a importância do uso e da proteção de dados pessoais para o desenvolvimento econômico, tecnológico e a inovação;
ii) Como a LGPD e outras normas aplicáveis, nacionais e internacionais, servem como bússola para que os dados pessoais possam ser utilizados para o desenvolvimento econômico, tecnológico e a inovação, de forma ética, segura e responsável?
iii) Quais práticas poderiam ser implementadas para melhorar a proteção de dados e segurança jurídica no tratamento de dados pessoais para o desenvolvimento econômico, tecnológico e a inovação?

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

5. Neste contexto, o IAB Brasil vem por meio deste documento atender a solicitação de contribuição frente ao referido GT, com pontos que entende pertinentes para o estudo, de forma a contribuir para o aperfeiçoamento da temática discutida e elaboração da Política Nacional de Proteção de Dados.

---

i) Casos práticos e dados estatísticos que demonstrem a importância do uso e da proteção de dados pessoais para o desenvolvimento econômico, tecnológico e a inovação

6. Primeiramente, o IAB relembra - de forma bastante resumida - que a publicidade digital personalizada tem como objetivo exibir anúncios relevantes e úteis, no momento adequado, para pessoas potencialmente interessadas nos produtos ou serviços anunciados. Isso é possível graças à análise da atividade online de consumidores ao longo do tempo, de forma a conhecer melhor seu comportamento e tentar inferir parte de suas preferências e de seus interesses.

7. A publicidade personalizada é essencialmente probabilística e não determinística: a análise da atividade online de determinado consumidor auxilia na construção de modelos estatísticos que apontam probabilidades relativas a potenciais preferências e interesses, que podem ou não se confirmar, conforme a qualidade das informações e se identificadas ou não.

8. Em um mercado de marketing e publicidade digital cada vez mais diverso, plural e orientado por dados, **o uso de dados pessoais tornou-se um viabilizador de oferta e do desenvolvimento de produtos e serviços de forma mais eficiente e de acordo com as preferências de cada público**. Considerando o amplo acesso à Internet pela maioria da população, o uso de dados pessoais pelo mercado de publicidade permite que as empresas de todos os portes econômicos tenham uma maior visibilidade das necessidades e interesses de seus públicos e suas necessidades, possibilitando a oferta de serviços e produtos gerais, de nicho e customizados que dificilmente seriam divulgados por meio da publicidade tradicional de TV, imprensa e jornais.

9. Especialmente por meio dos dados pessoais, o mercado de publicidade digital consegue entender alterações relevantes de consumo e mudanças de mercado abarcando mais amplamente a diversidade social e econômica do Brasil, ao ofertar produtos e serviços de forma personalizada e em linha com a necessidade e realidade de cada consumidor, amenizando a probabilidade de segregação de determinado público. A coleta e análise de dados, quando feita de forma ética, legal e transparente, permite a criação de experiências mais relevantes para o público-alvo.

10. É importantíssimo recordar que pequenos e médios empresários conseguem, por meio da publicidade digital, ter alcance idêntico ou superior a grandes marcas, justamente pela possibilidade de direcionar anúncios para o público-alvo específico. É por meio dessa publicidade, e naturalmente dos dados pessoais obtidos por meio delas, que estas empresas e/ou empreendedores entendem e direcionam mais adequadamente seus produtos e serviços que, consequentemente, influem na sua suficiência e crescimento econômico.

11. Assim, a publicidade personalizada traz diversos benefícios concretos a todos os participantes da cadeia de publicidade digital e ao próprio consumidor.

12. Da perspectiva do consumidor, a publicidade personalizada:

(i) possibilita sua exposição a uma gama de marcas, produtos, serviços e causas de seu interesse;
(ii) ajuda na comparação e substituição de produtos e serviços por outros equivalentes, muitas vezes a preços menores ou condições melhores;
(iii) aumenta seu poder de escolha e de barganha, em razão da multiplicidade de ofertas disponíveis;
(iv) economiza tempo e custos de transação, agilizando o processo de busca por produtos e serviços ideais às suas necessidades específicas;
(v) auxilia na aquisição de produtos e serviços de nicho que não são oferecidos localmente e que dificilmente são anunciados para o público de forma geral, ao contrário de bens e serviços para consumo de massa; e
(vi) permite a utilização, de forma gratuita e contínua, de conteúdos, aplicativos e serviços online custeados por publicidade.

13. Da perspectiva dos anunciantes, a publicidade personalizada:

(i) permite a empresas de qualquer lugar do mundo e dos mais diversos tamanhos a alcançarem consumidores potencialmente interessados em seus produtos e serviços específicos;
(ii) viabiliza que pequenos negócios façam publicidade de modo acessível e a custos baixos, alcançando consumidores que de outra forma dificilmente saberiam da existência de seus produtos ou serviços;
(iii) facilita às marcas criar conexões significativas com grupos de consumidores específicos, gerando confiança, engajamento, reciprocidade e valor; e
(iv) traz melhor retorno sobre o investimento, minimizando a exposição de consumidores a anúncios que não correspondam a seus interesses.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

14. Da perspectiva da sociedade, a publicidade personalizada:

(i) estimula o crescimento econômico, aumentando a eficiência e diminuindo os custos da publicidade e do marketing de modo geral.
(ii) aumenta a competição, permitindo que qualquer anunciante, independentemente de porte ou orçamento, tenha a oportunidade de alcançar consumidores interessados em seus produtos e serviços;
(iii) transforma um comércio ou uma indústria local em um ator econômico internacional, permitindo que milhões de consumidores de todo o mundo conheçam seus produtos e serviços;
(iv) representa em muitos casos a única alternativa para pequenos negócios fazerem publicidade, ante os elevados custos de anunciar em televisão, rádio ou imprensa;
(v) fortalece o jornalismo isento e independente, custeado por anúncios de interesse da audiência, por mais diversas que sejam suas preferências;
(vi) permite que produtos e serviços sejam oferecidos de forma individualizada e personalizada, e não apenas de maneira massificada;
(vii) viabiliza novos modelos de negócio, como o oferecimento em larga escala de conteúdos, aplicativos e serviços online gratuitos para grupos de consumidores, custeados por publicidade; e
(viii) possibilita que sites e veículos online democratizem a disponibilização de conteúdo, alcançando a maior quantidade possível de pessoas (e não somente quem poderia pagar pelo acesso ao conteúdo), apresentando informações relevantes e personalizadas de acordo com os interesses e preferências de cada indivíduo.

15. Importante ressaltar que os pontos sociais e econômicos acima comentados naturalmente impulsionam o terceiro ponto do questionamento do CNPD: desenvolvimento tecnológico. Neste aspecto, a gestão adequada dos dados pessoais pelas empresas movimenta e exige da área de tecnologia e segurança da informação uma constante melhoria de processos, procedimentos e ferramentas de proteção.

16. Estes três aspectos conjuntamente fortalecem as relações de confiança entre consumidores e as mais diversas empresas do mercado (e não somente de publicidade e marketing), incentivando interações e transações mais seguras, o que é fundamental para um bom e mais estável desenvolvimento social, cultural e econômico de médio e longo prazo.

ii) Como a LGPD e outras normas aplicáveis, nacionais e internacionais, servem como bússola para que os dados pessoais possam ser utilizados para o desenvolvimento econômico, tecnológico e a inovação, de forma ética, segura e responsável?

17. A LGPD, o GDPR e outras regulamentações similares aplicáveis desempenham um papel estratégico na orientação do uso de dados pessoais de forma ética, responsável e alinhada às expectativas do mercado. Para o setor de marketing e publicidade, essas normas vão além da obrigatoriedade regulatória, apresentando-se como uma oportunidade para construir uma relação de confiança junto aos consumidores e parceiros de negócios. Ao estabelecer princípios como transparência, necessidade e segurança, a LGPD cria um ambiente de negócios mais previsível e confiável, essencial para o desenvolvimento sustentável do setor.

18. Do ponto de vista do IAB, empresas que demonstram *compliance* com a LGPD destacam-se pela adoção de boas práticas e demonstram prezar pela sua reputação, posicionando-se como líderes no mercado ao fortalecer a relação de confiança com seus consumidores e parceiros de negócios. Essa adequação é percebida como um diferencial competitivo, gerando maior segurança jurídica, reduzindo riscos financeiros e consolidando a reputação corporativa.

19. Assim, a LGPD funciona como uma bússola para guiar empresas no uso responsável dos dados. Esse alinhamento entre regulamentação e melhores práticas empresariais promove o desenvolvimento de um ambiente de negócios mais ético e sustentável em um competitivo setor de marketing e publicidade.

20. No entanto, entre os principais pontos de atenção está a complexidade normativa, que muitas vezes exige das empresas investimentos consideráveis em tecnologia, consultoria jurídica e treinamento interno para garantir conformidade. Esse cenário pode representar um fardo desproporcional para pequenas e médias empresas, que possuem menos recursos para se adaptar às exigências da lei.

21. Outro ponto crítico reside na falta de clareza em alguns aspectos regulatórios específicos, como os critérios para o reconhecimento de perfilamento ou a identificação de dados pessoais na cadeia de publicidade personalizada. Isso gera incertezas, especialmente quando a capacidade de identificar o titular é restrita a um único ente dessa cadeia, levantando questionamentos sobre a caracterização de um dado como pessoal em situações de identificabilidade limitada.

22. Assim, embora existam pontos a serem aprimorados e interpretados pela autoridade competente e ordenamento jurídico, do ponto de vista do IAB, a LGPD conjuntamente com

as resoluções específicas da Autoridade Nacional de Proteção de Dados ("ANPD") estabelecem uma base sólida que beneficia tanto empresas quanto consumidores.

iii) Quais práticas poderiam ser implementadas para melhorar a proteção de dados e segurança jurídica no tratamento de dados pessoais para o desenvolvimento econômico, tecnológico e a inovação?

23. Um dos principais desafios enfrentados pelas empresas é a complexidade regulatória, que frequentemente demanda altos investimentos em tecnologia, consultoria jurídica especializada e programas de capacitação interna para alcançar a conformidade. Para pequenas e médias empresas, especialmente, essas exigências podem se tornar um obstáculo significativo, dado o orçamento mais limitado e os recursos restritos para implementar mudanças estruturais.

24. Do ponto de vista do IAB, a **harmonização de normas** pode ser um caminho para promover um ambiente regulatório mais coeso e eficiente no tratamento de dados pessoais. Isto é, adotar regras alinhadas com práticas reconhecidas internacionalmente, naturalmente considerando a tipicidade e particularidade do mercado brasileiro, pode auxiliar o Brasil a se posicionar como um ambiente confiável para negócios globais, atraindo investimentos estrangeiros e ampliando a competitividade das empresas locais.

25. Adicionalmente, o IAB acredita que a **uniformização e definição de boas práticas setoriais** desempenha um papel crucial na aplicação prática das normas tendo em vista a sensibilidade e criticidade de cada mercado. Ainda nesse sentido, é essencial que sejam ouvidos os representantes dos diversos setores da sociedade e efetivamente adotar diretrizes oportunamente propostas por estes.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANEXO XIII – CONTRIBUIÇÕES: INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS (INPD)

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

INPD
INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS

Ofício DIREX n° 10/2024

Curitiba/PR, 01 de dezembro de 2024

À

Presidência do CNPD

A/C: Sra. Lilian Manoela Monteiro Cintra de Melo – Conselho Nacional de Proteção de Dados – CNPD

A/C: Sr. Rony Vainzof – Conselheiro Titular e Coordenador do GT5

Ref.: Solicitação de Contribuição ao CNPD (GT5)

Prezado(a) Sr.(a). Presidente e Coordenador,

Em atenção ao Ofício recebido, agradecemos a oportunidade de contribuir com os trabalhos do GT5 no desenvolvimento de subsídios relacionados ao uso de dados pessoais para o desenvolvimento econômico, tecnológico e de inovação, nas diversas temáticas mencionadas no referido documento.

Optamos por abordar, em nossa contribuição, o tema **"Uso de Dados Pessoais para a Prevenção à Fraude e Segurança"**, considerando sua relevância no contexto atual de segurança, inovação e desenvolvimento econômico.

Abaixo, apresentamos nossas reflexões e considerações, levando em conta a importância desse tema para o ambiente econômico e de inovação, tanto no cenário nacional quanto internacional. Ressaltamos, ainda, a necessidade de observar as normas legais pertinentes, incluindo, mas não se limitando, às leis de proteção de dados pessoais.

Reiteramos nosso comprometimento com os objetivos do GT5 e permanecemos à disposição para eventuais esclarecimentos ou aprofundamentos que se façam necessários.

Atenciosamente,

Martha Leal
Vice-Presidente do INPD

Rafael Reis
Presidente INPD

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

INPD INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS

Sumário

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

INPD INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS

Contribuições do INPD ao CNPD: Proposta sobre Dados Pessoais e Prevenção à Fraude

1. Introdução

Primeiramente, importante registrar para contextualização das considerações abaixo expostas, que o tema selecionado para fins de abordagem nos termos do ofício recebido é o uso de dados pessoais para fins de prevenção à fraude e segurança.

Sendo assim, a considerar o cenário nacional em que estamos inseridos, nos dirigimos imediatamente à Lei Geral de Proteção de Dados -LGPD, especialmente, aos princípios estabelecidos pelo art. 6º., com especial ênfase, ao inciso I, e que estabelece que toda e qualquer atividade de tratamento de dados pessoais requer uma finalidade legítima e específica, além de devidamente informada ao titular.

Pois bem, sabemos que a finalidade de um tratamento impacta significativamente na escolha da hipótese legal que autoriza o respectivo tratamento de dados, tornando indispensável que os controladores tenham a ciência da responsabilidade que atraem, se porventura, utilizarem finalidades diversas daquelas que, de fato, alicerçam a escolha de uma das bases legais do art.7º. ou 11º. da LGPD.

E, sendo a temática ora eleita para fins de estudo e sugestões de contribuições ao CNPD, o uso dos dados para fins de prevenção à fraude e segurança, nos endereçamos ao art. 11º., "g" que trata da garantia da prevenção à fraude e segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

Tratando-se, pois, de dados pessoais sensíveis, o processamento destes dados para fins de diligência na contenção de práticas fraudulentas e à própria segurança do titular, é indispensável por parte dos controladores, a observância aos outros princípios legais, como a adequação, necessidade e qualidade dos dados, bem como, o dever de transparência, responsabilização, de prover segurança, de prevenção e de não discriminação.

No material elaborado, são apresentados diversos setores que utilizam os dados pessoais para a mesma finalidade, ou seja, de prevenção à fraude e segurança. Entretanto, não se pretendeu desta maneira exaurir todos os tipos de tratamentos realizados, eis que seria impossível, dada a velocidade do desenvolvimento das tecnologias o que impõe a exigência da mesma celeridade, por parte dos controladores, no implemento de medidas eficientes no combate aos desafios postos e que demandam implementos para proteger fraudes, sob pena de prejuízos inimagináveis no sistema financeiro e econômico.

Afinal de contas, sem a confiança dos consumidores, um mercado pode sucumbir e é essa justamente a relevância da hipótese autorizadora de tratamento de dados pessoais (art. 11, G) que ora se enfrenta.

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

INPD INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS

No âmbito do Sistema Financeiro, as instituições financeiras operam somente através de autorização do Banco Central do Brasil e são regulados por suas normas, além das normas legais comuns a todos, tais como, a Constituição Federal, Código Civil, Código de Defesa do Consumidor, Marco Civil da Internet e Lei Geral de Proteção de Dados.

No que tange ao tratamento de dados pessoais por parte das instituições financeiras e Instituições de Pagamento, o BCB, possui as seguintes normas e resoluções, as quais, os agentes de tratamento envolvidos com os dados pessoais, devem obedecer, além das demais leis já referidas.

As principais são:

- Resolução no. 4.893, de 26/02/2021, que dispõe sobre a Política de Segurança Cibernética e os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.
- Circular no. 3.978, de 23/01/2020, estabelece procedimentos e controles internos a serem adotados pelas instituições financeiras para prevenção de crimes de lavagem de dinheiro e financiamento ao terrorismo. Políticas de "Conheça o seu Cliente" (KYC)
- Resolução no. 142, de 23/09/2021, dispõe sobre procedimentos e controles de prevenção de fraudes na prestação de serviços de pagamento. As instituições devem estabelecer limites para transações, manter registros detalhados de ocorrências de fraudes.
- Resolução Conjunta no. 6, de 23/05/2023, estabelece requisitos para compartilhamento de dados e informações sobre indícios de fraudes entre instituições financeiras.

No panorama do mercado de seguros, há a necessidade das empresas de seguro vincularem-se à Superintendência de Seguros Privados (SUSEP), órgão regulador do mercado securitário e que estabelece normativas que abordam o tratamento de dados pessoais no setor, em conformidade com a Lei Geral de Proteção de Dados (LGPD).

As principais são:

- Circular SUSEP no. 638/2021: Define requisitos mínimos de segurança cibernética para assegurar a proteção de dados pessoais tratados pelas seguradoras, entidades abertas de previdência complementar, sociedades de capitalização e resseguradores.
- Resolução CNSP no. 450/2022: Estabelece requisitos para credenciamento e funcionamento das sociedades processadoras de ordem do cliente, enfatizando condutas no relacionamento com este.
- Circular SUSEP no. 612/2020: Estabelece diretrizes para a prevenção à lavagem de dinheiro e ao financiamento ao terrorismo no setor de seguros.

No panorama internacional, especialmente no europeu, temos o Regulamento Geral de Proteção de Dados, que em seu art. 6 (1) (f), permite o tratamento de dados pessoais

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

para fins de prevenção à fraude ancorado na base legal do legítimo interesse do controlador.

O princípio da minimização de dados, que determina que somente os dados necessários devem ser coletados e tratados tem de ser respeitado por parte dos controladores, bem como, técnicas como anonimização e pseudonimização, as quais são altamente recomendadas devem ser implementadas.

Na União Europeia, o OLAF (Organismo Europeu e Luta Antifraude) foi criado em 1999 para reforçar o combate à fraude e à corrupção. O seu trabalho está alinhado ao Tratado da União Europeia (TFUE), que define a proteção dos interesses financeiros da EU como prioridade. Embora seja parte da Comissão Europeia, a OLAF opera de forma independente no que se refere a investigações. O seu objetivo é garantir transparência e responsabilidade na gestão de recursos financeiros da União Europeia.

Resumidamente, o seu trabalho é investigar, detectar e combater fraudes relacionadas aos recursos financeiros, combatendo irregularidades e má gestão dos recursos, além de promover políticas antifraude em toda a União Europeia.

A Comissão Europeia possui diversas recomendações sobre o tema estabelecendo estratégias para o uso de dados na prevenção e combate à fraude e recomenda que os Estados Membros adotem e revisem estratégias nacionais antifraude, integrando ferramentas informáticas específicas na luta contra a fraude, reforçando a análise do risco.

No que tange a importância do uso dos dados pessoais para fins de proteção à fraude e segurança, não podemos nos olvidar dos fundamentos da Lei Geral de Proteção de Dados, os quais estão elencados no art. 2º., e que sinalizam os valores aos quais a norma pretende proteger.

Nessa linha de raciocínio, o desenvolvimento econômico e tecnológico e a inovação estão devidamente referenciados no dispositivo legal referido, em seu inciso V, e vem ao encontro das finalidades em que os mais diversos usos de dados se dá sob a hipótese legal do art. 11, G, da LGPD.

Por fim, o uso de dados pessoais para prevenção à fraude oferece benefícios significativos ao integrar inovação e economia, pois permite a detecção de padrões de comportamentos anômalos em tempo real, reduzindo riscos de fraudes financeiras e cibernéticas. Ao promover a minimização de riscos, fortalece a segurança das transações digitais, incentivando a confiança dos consumidores em ambientes online. Permite maior eficiência operacional, ao diminuir custos com investigações e processos manuais, e, derradeiramente, contribui para a proteção das empresas e consumidores, estimulando a confiança na economia.

Além da utilização de dados pessoais para prevenção à fraude e segurança, destaca-se um tema cada vez mais relevante: a proteção de dados no uso de tecnologias para **monitoramento de empregados em regimes de teletrabalho**. A adoção massiva do teletrabalho, acelerada pela pandemia da Covid-19, trouxe novos desafios quanto ao equilíbrio entre o poder de controle do empregador e a privacidade

dos trabalhadores, especialmente diante do uso crescente de ferramentas de vigilância e monitoramento remoto.

Diante disso, este material apresenta sugestões voltadas a enfrentar esses desafios e estabelecer melhores práticas, alinhadas à Lei Geral de Proteção de Dados (LGPD) e demais legislações aplicáveis. O objetivo é propor diretrizes que assegurem transparência no uso de tecnologias de monitoramento, proporcionalidade na coleta e tratamento de dados pessoais e respeito aos direitos fundamentais à privacidade e à dignidade dos empregados, promovendo um ambiente de trabalho justo e seguro.

1.1. Elaboração e Contribuições dos Autores

Este estudo foi desenvolvido com a valiosa contribuição de membros do Instituto Nacional de Proteção de Dados (INPD), cujas expertises abrangem áreas fundamentais para a análise dos temas tratados. Agradecemos especialmente:

- **Martha Leal**: Vice-Presidente do INPD, Presidente da Comissão de Inteligência Artificial e da Comissão de Comunicação, cuja visão estratégica e conhecimento sobre inovação tecnológica foram essenciais para a construção deste material.
- **Atilio Braga**: Presidente da Comissão de Governança e Compliance e Secretário Geral do INPD, que trouxe contribuições indispensáveis relacionadas à conformidade e governança de dados.
- **Rafael Mosele**: Diretor Financeiro e Presidente da Comissão de Direito do Trabalho, responsável por enriquecer o estudo com uma abordagem aprofundada sobre a proteção de dados no contexto laboral.

A dedicação e o compromisso desses profissionais garantiram a qualidade e a relevância do conteúdo aqui apresentado, promovendo um estudo abrangente e alinhado às melhores práticas nacionais e internacionais em proteção de dados e prevenção de fraudes.

2. Setor Financeiro e Bancário

O setor financeiro e bancário depende do tratamento de dados pessoais para fins de detecção de fraudes, sendo fundamental para proteger instituições, clientes e o ecossistema financeiro contra prejuízos decorrentes de ataques cibernéticos e violações de segurança.

O tratamento de dados pessoais, neste cenário e para essa finalidade, garante confiabilidade das transações, minimiza riscos e cumpre exigências regulatórias.

2.1. Exemplos de tratamentos no setor financeiro e bancário:

2.1.1. Análise de Transações:

Instituições financeiras utilizam sistemas de inteligência artificial para monitorar padrões de comportamento de transações financeiras. Os dados pessoais como

localização, horários e valores de transações ajudam a identificar atividades atípicas, sinalizando possíveis fraudes em tempo real.

Caso prático: Uma fraude em cartão de crédito pode ser detectada por uso simultâneo em dois países diferentes ao mesmo tempo, levando ao bloqueio do cartão até a confirmação da operação pelo titular.

2.1.2. Autenticação Biométrica:

Utilização de biometria através de impressão digital, reconhecimento facial ou voz, para autenticar usuários em aplicativos, garantindo que apenas o titular tenha acesso à conta.

Caso prático: Reconhecimento facial ou digital para liberação de transferências acima de determinado valor.

2.1.3. Triagem de crédito e contratação de produtos

As informações fornecidas em solicitações de abertura de conta ou requerimento de crédito passam por uma triagem, cujos dados são cruzados com bases públicas e/ou internas para identificar inconsistências ou fraudes documentais.

2.1.4. Prevenção de lavagem de dinheiro

As instituições financeiras são obrigadas por força de normas regulatórias advindas do Banco Central do Brasil – BCB-, a monitorar transações de alto valor ou repetitivas para identificar atividades suspeitas.

Caso prático: Um indivíduo tem os seus dados cruzados com listas de vigilância de clientes politicamente expostos (PEPs) ou de indivíduos sob sanções para fins de análise sobre possível concessão de crédito solicitado.

2.1.5. Detecção de fraudes em transferências bancárias

As instituições financeiras monitoram as transferências, através do uso de tecnologias avançadas e processos automatizados para fins de detecção e bloqueio de atividades suspeitas. Esse monitoramento dos dados pessoais utiliza padrões de comportamento, análise de dados transacionais e integração com bases de dados externas para garantir segurança.

Caso prático: A instituição financeira, através do seu sistema , analisa os dados do remetente e do destinatário, tais como, nome, CPF/CNPJ, número da conta e banco, dados da transação, como valor, data, hora, finalidade e canal de operação (app, internet banking, caixa eletrônico, etc.), informações do dispositivo, tais como, o modelo,

sistema operacional, endereço de IP e geolocalização, e, o histórico do cliente, para comparação com os padrões de transferência anteriores e frequência de movimentações.

2.1.6. Bloqueio ou retenção de transações suspeitas

As transações eventualmente sinalizadas como suspeitas podem ser bloqueadas, até o término da conclusão da análise, bem como, retidas de forma manual, por uma equipe de especialistas que avalia se a transação é legítima.

2.1.7. Registro e auditoria

As instituições financeiras por força regulatória armazenam os "logs" de todas as transações, incluindo as suspeitas e os motivos de bloqueio, para auditoria futura.

Os dados coletados ajudam a refinar os algoritmos e atualizar as regras de monitoramento.

2.1.8. Implementação de medidas de segurança para evitar vazamento de informações

O sistema financeiro requer a implementação de medidas de segurança por parte das instituições financeiras para fins de mitigação de riscos envolvendo dados pessoais dos titulares. O Banco Central do Brasil, órgão regulador, estabelece diretrizes para que as instituições financeiras assegurem a proteção dos dados pessoais de seus clientes. Essas orientações estão alinhadas à Lei Geral de Proteção de Dados Pessoais – LGPD- e visam garantir a segurança e a privacidade das informações no âmbito do Sistema Financeiro Nacional.

Caso Prático[1]: Em janeiro de 2002, o BCB, informou um vazamento de dados de aproximadamente 160 mil chaves PIX vinculadas à empresa Acesso Soluções de Pagamento, instituição de pagamento autorizada. As informações vazadas incluíam dados cadastrais como nome, CPF e dados bancários. A causa do incidente se deu em função do sistema de acesso de permissões de usuários não autorizados.

3. E-commerce

[1] https://g1.globo.com/economia/pix/noticia/2022/02/03/pix-quais-dados-foram-vazados-quais-os-riscos-e-como-se-proteger.ghtml?UTM_SOURCE=outlook&UTM_MEDIUM=share-bar-app&UTM_CAMPAIGN=materias

https://www-correiobraziliense-com-br.cdn.ampproject.org/c/s/www.correiobraziliense.com.br/cidades-df/2024/11/amp/6993331-pcdf-bloqueia-rs556-mil-de-quadrilha-especializada-em-golpes-cibernéticos.html

O uso de dados pessoais para prevenção à fraude no e-commerce é de grande relevância para garantia da segurança das transações, proteção dos consumidores, evitando assim, prejuízos financeiros às empresas. A manutenção da confiança dos consumidores permite o crescimento da economia, uma vez que, sentem-se seguros na utilização dos sistemas. Por sua vez, a minimização de perdas financeiras, causados por prejuízos em decorrência de "Chargeback", devoluções fraudulentas e uso indevido de cupons produzem maior segurança jurídica aos atores que atuam neste mercado.

3.1. Exemplos:

3.1.1. Prevenção à Fraudes em Pagamentos Online

A utilização de dados pessoais, como endereços de IP, histórico de compras e geolocalização são importantes para que as plataformas de e-commerce identifiquem compras fraudulentas.

Caso prático: O bloqueio de uma transação através de bloqueio de sistema quando for realizada por um dispositivo nunca utilizado e proveniente de uma região de alto risco.

Caso Prático[2]: Em 2019, a empresa de e-commerce Netshoes enfrentou um incidente de segurança que resultou na exposição de dados de 2 milhões de clientes na internet, incluindo nome completo, CPF, e-mail e histórico de compra.

Caso Prático[3]: Em outubro de 2021, uma falha de segurança na plataforma brasileira Hariexpress expôs mais de 1,7 bilhão de dados de clientes e lojistas cadastrados em sites de comércio eletrônico.

3.1.2. Análise comportamental de usuários

Com base no histórico do cliente, o sistema identifica os padrões normais de transações, frequência, valores e tipos de produtos possibilitando a identificação de anomalias que apontam para possíveis fraudes.

3.1.3. Verificação de identidade

As plataformas podem exigir a depender do valor da transação, validação adicional do usuário. Exemplo clássico desta situação se dá quando é requerido ao consumidor/titular de dados pessoais, uma selfie acompanhada do documento de identidade para validação da sua identidade.

3.1.4. Controle de fraudes em cupons e promoções

[2] https://g1.globo.com/tecnologia/noticia/2024/07/17/netshoes-diz-que-dados-de-clientes-podem-ter-sido-vazados-apos-incidente-cibernetico.ghtml

[3] https://exame.com/tecnologia/entenda-caso-hariexpress-megavazamento/

As plataformas para fins de coibir fraudes com a utilização de múltiplas contas para cupons ou promoções, processam dados pessoais como IP, dispositivos usados, e-mails e método de pagamento.

Caso Prático: um cliente criando várias contas e usando o mesmo dispositivo para obtenção de descontos repetidamente poderá ter a sua conta bloqueada.

3.1.5. Rastreamento de logística e entregas

As plataformas em seus sistemas de disputas on-line (ODRs) seguidamente são demandadas por reclamações envolvendo fraudes relacionadas a falsas reclamações de não recebimento de produtos. O uso de rastreamento em tempo real, endereço de entrega e análise do histórico de compras e reclamações anteriores para validar se um cliente recebeu ou não o produto é de suma importância para a resolução da reclamação.

3.1.6. Prevenção de fraudes de reembolso e Chargeback

As plataformas seguidamente estão envolvidas com reclamações de clientes mal-intencionados que solicitam reembolsos indevidos alegando que não autorizaram as compras. Nesses casos, sistemas verificam se o dispositivo utilizado na compra é o mesmo que o cliente geralmente utiliza em suas transações, bem como, geolocalização, histórico de compras e métodos de pagamento.

Portanto, evita-se através da análise dos dados pessoais do consumidor/titular destes dados, que empresas sejam prejudicadas com cancelamento e devoluções de valores, as quais não deram causa.

3.1.7. Validação de dados de cadastro

As plataformas precisam validar o cadastro de dados realizados para fins de identificar incorreções que possam gerar fraudes, incluindo a lavagem de dinheiro. Nesse sentido, os sistemas identificam se o CPF informado no cadastro é válido e associado ao nome e endereço fornecido pelo indivíduo.

4. Companhias Aéreas:

O tratamento de dados pessoais no setor das companhias aéreas com a finalidade de prevenção à fraude e de segurança é uma prática comum, devido a necessidade de garantir a segurança dos passageiros e o cumprimento de normas regulatórias.

4.1. Exemplos:

4.1.1. Verificação de identidade no Check-In

As companhias aéreas utilizam sistemas de validação de identidade para verificar os dados dos passageiros no momento do check-in. Informações pessoais, como nome, número do passaporte ou documento de identificação, são cruzadas com bancos de dados governamentais ou listas de vigilância para prevenir atividades fraudulentas ou ameaças à segurança.

4.1.2. Análise de transações

As companhias aéreas analisam dados de compra online, tais como, pagamentos realizados com cartões de créditos roubados, múltiplas passagens compradas com o mesmo cartão para destinos diferentes em um curto espaço de tempo.

4.1.3. Análise de atividades suspeitas

As companhias aéreas analisam dados como endereço de IP, geolocalização, e histórico de compras são utilizados para identificação de atividades suspeitas.

4.1.4. Verificação de dados pessoais para consulta em listas de proibição de passageiros (Uso de APIs para Screening)

Os dados dos passageiros são enviados para verificação em listas de restrição, como a No-Fly List, nos EUA. Os dados do passageiro são comparados com listas de terroristas, criminosos procurados ou pessoas com proibições legais de viajar. Essa troca de informações ajuda a identificar pessoas que representam riscos à segurança antes do embarque.

**Screening* é o processo de verificação ou triagem de informações para identificar riscos, irregularidades ou inconsistências em um determinado contexto. Os dados são coletados, cruzados, analisados manual ou automaticamente e é tomada uma decisão com base no resultado do *Screening*.

4.1.5. Reconhecimento Facial e Biométrico

Muitas Companhias Aéreas implementam tecnologias de reconhecimento facial e biometria no embarque e no controle de fronteiras. O objetivo é comparar as imagens capturadas com os dados armazenados em passaportes biométricos e bancos de dados governamentais para prevenir fraudes de identidade e consequentemente prática de crimes.

4.1.6. Monitoramento de comportamentos em aeroportos

Os aeroportos, utilizam sistemas de segurança dentro destes espaços, com câmeras e inteligência artificial para monitorar o comportamento de passageiros, com o objetivo de detectar preventivamente comportamentos anormais e consequentes riscos à segurança.

4.1.7. Gestão de Bagagem

Informações vinculadas ao registro de bagagens para evitar fraudes, como o uso de etiquetas falsas para retirar pertences de outro passageiro ou possibilitar a troca proposital de bagagem. Algumas companhias aéreas utilizam QR Codes ou tecnologia RFID para rastrear bagagens associadas a dados específicos do cliente.

4.1.8. Programas de Fidelidade

Dados pessoais de clientes inscritos em programa de fidelidade são analisados para identificar possíveis fraudes, como transferências de milhas não autorizadas ou uso indevido de benefícios.

4.1.9. Prevenção de Ataques Cibernéticos

Companhias aéreas monitoram atividades nos sistemas de reservas e contas de usuários para prevenir roubo de dados pessoais ou informações financeiras. Autenticação de identidade e análise comportamental são usados para identificar tentativas de acesso não autorizadas.

Caso Prático[4]: A LATAM Airlines, em 2021, informou que parte dos membros de seu programa de fidelidade, o LATAM Pass, teve dados pessoais expostos devido a um ataque cibernético sofrido pela empresa de tecnologia SITA, que prestava serviços ao setor aéreo.

5. Mercado de Seguro:

O tratamento de dados pessoais no ramo de seguros detém importância significativa, uma vez que fraudes neste ambiente, podem gerar prejuízos milionários para as empresas, bem como, aos segurados. A análise de dados pessoais permite a identificação de comportamentos suspeitos, reduzindo pagamento indevido de indenizações fraudulentas.

As seguradoras também são obrigadas por regulamentações específicas do Órgão Regulador, a SUSEP, a adotar medidas de segurança e prevenção à fraude, além, das obrigações impostas pela Lei Geral de Proteção de Dados. Menores custos operacionais, preços mais competitivos, maior precisão na análise de sinistros e desenvolvimento de produtos personalizados, são alguns dos benefícios do tratamento de dados pessoais para fins de prevenção à fraude e segurança.

5.1. Exemplos:

5.1.1. Detecção de Fraudes em Sinistros

[4] https://valor.globo.com/empresas/noticia/2021/03/13/ataque-hacker-expe-dados-de-passageiros-da-latam-no-brasil.ghtml

As seguradoras analisam os dados pessoais, histórico de sinistros e padrões de comportamento para identificar possíveis fraudes em pedidos de indenização.

- Emissão de Apólices Falsas

Criminosos utilizam dados pessoais obtidos ilegalmente para emitir apólices de seguros fraudulentas, cobrando prêmios sem cobertura válida.

- Solicitações de contratos e boletos fraudulentos

Fraudadores se passam por corretores de seguros, utilizando dados pessoais roubados para enviar contratos e boletos falsos aos consumidores. Ao pagar por esses documentos. As vítimas acreditam estar contratando um seguro legítimo, mas acabam sendo lesadas financeiramente.

Caso Prático[5]: Em abril de 2023, foi reportado um vazamento que expôs mais de 5,8 milhões de registros de saúde de brasileiros, incluindo consultas, procedimentos e exames realizados por uma importante seguradora nacional. As informações abrangiam dados pessoais como nomes, CPFs, data de nascimento, e detalhes de planos de saúde entre 2016 e 2020. O vazamento de dados foi atribuído a empresa Porto Saúde.

Caso Prático[6]: Em novembro de 2020, a seguradora Prudential do Brasil comunicou um incidente de segurança que permitiu que uma pessoa não autorizada copiasse informações relacionadas a propostas de contratação de serviços, resultando no vazamento de dados pessoais de clientes.

6. Tecnologia e Mídias Sociais:

O tratamento de dados pessoais para fins de prevenção à fraude na tecnologia e nas mídias sociais é de suma importância para proteger usuários, plataformas e anunciantes contra atividades maliciosas e fraudulentas, como o roubo de identidade, criação de contas falsas e golpes financeiros.

Esse tratamento contribui para a confiança nas plataformas e para a segurança dos seus usuários e das interações que ocorrem nestes ambientes virtuais. O objetivo é proteger o usuário, procurando impedir que sejam vítimas de golpes, como phishing, roubo de contas ou fraudes financeiras, entre outros, reduzindo perdas financeiras, por fraude publicitária, roubo de serviços ou uso indevido das funcionalidades.

Promove-se, assim, o aumento da confiabilidade de um ambiente digital e seguro, essencial para a continuidade das operações e engajamento dos usuários.

[5] https://canaltech.com.br/seguranca/vazamento-expoe-quase-6-milhoes-de-dados-de-saude-dos-brasileiros-246314/
[6] https://www.cisoadvisor.com.br/seguradora-prudential-tem-dados-roubados-em-ciberataque/

6.1. Exemplos:

6.1.1. Autenticação de identidade para detecção e bloqueio de contas falsas

As plataformas como Facebook, Google, Instagram, Microsoft fazem uso de dados pessoais, tais como, números de telefone, reconhecimento facial, verificação em duas etapas, para assegurar sobre a identidade do usuário e prevenir fraudes, através da sua autenticação segura.

Caso Prático: O bloqueio de contas por detecção de tentativas de acesso a partir de dispositivos e localização não reconhecidos.

Caso prático: Uma conta que interage em massa com milhares de perfis em minutos pode ser bloqueada por apresentar comportamento típico de "bots".

6.1.2. Prevenção de fraude publicitária

As plataformas monitoram curtidas e impressões de anúncios para identificar "click fraude", cliques maliciosos feitos por "bots" ou concorrentes, processando dados pessoais como endereço de IP, dispositivos, geolocalização e padrões de curtidas.

- Combate ao "phishing" e links maliciosos

Os links compartilhados em mensagens e postagens são analisados para identificar conteúdos fraudulentos, evitando assim, que os usuários sejam vítimas de golpes financeiros.

Caso prático: Um usuário envia um link que redireciona a uma página falsa de login, terá esse link bloqueado pelo Instagram, mesmo que seja feito através de uma mensagem direta.

-Análise comportamental dos usuários

As plataformas sociais utilizam inteligência artificial para identificar comportamentos fora do padrão, como curtidas ou comentários em massa.

Caso prático: Um usuário começa a seguir milhares de perfis em minutos. A conta é temporariamente bloqueada até posterior confirmação de identidade deste.

- Monitoramento de conteúdo e comentários

Os comentários e postagens são analisados pelo sistema com inteligência artificial para identificar "spam" ou conteúdos que possam envolver fraudes, discurso de ódio e inúmeros outros ilícitos.

Caso prático: As plataformas através da análise de textos das postagens, frequência de publicação e padrões linguísticos do usuário, podem excluir links repetidos para promoções falsas.

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

7. Setor Público:

O tratamento de dados pessoais para prevenção à fraude no setor público é de grande relevância para fins de garantir a integridade dos recursos públicos, evitar desvios financeiros, proteger cidadãos e promover a transparência nos serviços governamentais.

A fraude no setor público é de extrema nocividade pois além de prejuízos econômicos, abala a confiança da sociedade e compromete os programas sociais.

7.1. Exemplos:

7.1.1. Prevenção de Fraudes em Benefícios Sociais

Os dados dos indivíduos são processados e analisados pelo Governo para análise de informações de beneficiários para identificar inconsistências ou informações duplicadas.

Caso Prático: Programas de combate a fraude no INSS, que cruzam informações para evitar pagamentos indevidos de pensões ou aposentadorias.

7.1.2. Detecção de fraudes em licitações

Os sistemas monitoram concorrências públicas para identificar irregularidades, como vínculos entre empresas participantes, através da participação societária dos sócios.

7.1.3. Prevenção de fraude em impostos

O setor público, através de seus órgãos fiscais, como a Receita Federal, cruza informações para identificar inconsistências em declarações de renda ou pagamentos tributários a menor.

Caso prático: A detecção de incompatibilidade entre a renda declarada e o patrimônio do contribuinte, através do cruzamento de informações, como renda declarada, movimentação bancária e patrimônio.

7.1.4. Monitoramento de fraudes em programas habitacionais

O setor público analisa dados dos candidatos a programas como o "Minha Casa Minha Vida" para evitar fraudes, como a inclusão de pessoas com imóveis próprios, situação vedada para a concessão deste programa.

Caso prático: Os dados de um candidato a obtenção de um financiamento pela modalidade do programa "Minha Casa Minha Vida" são analisados e verificados em cartórios para confirmar a inexistência de propriedade em nome do solicitante, ratificando assim a sua elegibilidade.

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

8. Compartilhamento de Dados Pessoais para o fim de combater fraudes

Considerando que o compartilhamento de dados pessoais para fins de combater e mitigar fraudes em vários seguimentos, pode ser um meio idôneo e legítimo, entretanto, que merece atenção para que se evite o uso indevido destes dados.

Deste modo, recomenda-se que uma Política Nacional de Tratamento e Processamento de dados pessoais com o fim de verificação de fraudes deva observar rigorosamente os princípios da **necessidade**, **finalidade**, e **proporcionalidade**, conforme previsto na Lei Geral de Proteção de Dados (LGPD).

Este racional visa garantir que os dados pessoais compartilhados sejam utilizados exclusivamente para a prevenção e o combate a fraudes, prevenindo desvios de finalidade e garantindo a proteção dos direitos dos titulares.

9. Proteção de dados e uso da tecnologia no monitoramento do empregado no teletrabalho

9.1. Introdução

Nas relações de trabalho, assim como em outras tantas áreas, a coleta e combinação de dados de diferentes fontes representa elevado risco à proteção de dados, na medida em que o uso da tecnologia se faz diuturnamente presente no curso do contrato de trabalho.

Ainda que na relação pura da prestação de serviços pelo empregado não se tenha por escopo final a coleta de dados, tal acaba por ocorrer, desde a sua candidatura a vaga de emprego, durante todo o período de vínculo empregatício até após a ruptura do contrato de trabalho.

O uso da tecnologia no mundo do trabalho ao mesmo tempo que é essencial à persecução dos interesses das empresas, também acaba por ser cada vez mais invasiva e abrangente, do que são meros exemplos sistemas biométricos de registro de entrada e saída das organizações, registro biométrico da jornada, câmeras de segurança, câmeras de dispositivos eletrônicos para o desenvolvimento do trabalho à distância e a geolocalização de veículos da empresa.

E quando se trata de dados pessoais, estes não só estão sujeitos à proteção, como também representam risco de violação aos direitos da personalidade, na medida em que o equipamento de trabalho não só representa o meio de execução da atividade, como, do mesmo modo, pode ser o instrumento utilizado para o controle.

Esta potencial invasão de privacidade ao mundo dos trabalhadores, porém, poderá ser acautelada pela Lei Geral de Proteção de Dados (LGPD) aliada às demais legislações nacionais relativas ao direito do trabalho e à proteção de dados, a exemplo da própria Constituição Federal (CF) e da Consolidação das Leis do Trabalho (CLT).

Nesse contexto, é que a vigilância à distância, o monitoramento de correio eletrônico e a geolocalização tomam especial importância no contexto laboral, especialmente no Brasil, onde essas questões não são detalhadas com suficiência, atraindo a necessidade de se estabelecer uma governança da privacidade dentro das organizações, criar regulamentos internos, políticas e manuais de boas práticas capazes de impor limites, mas acima de tudo, defender os interesses de controladores (empregadores) e titulares de dados (empregados).

9.2. Teletrabalho e vigilância à distância

A pandemia da Covid-19, a crise de saúde pública e as medidas de isolamento impostas por autoridades de saúde, aceleraram sobremaneira a adoção do teletrabalho pelas organizações. Esta mudança provocada pela pandemia acarretou o reconhecimento pela sociedade quanto às facilidades e benefícios da utilização de novas ferramentas de colaboração e comunicação online.

É bem verdade que, nesse cenário, o uso da tecnologia desencadeou um conjunto de riscos para a privacidade dos trabalhadores, dos seus familiares, bem como para o próprio empregador e para a informação e dados, que se tornaram vulneráveis, pelo tratamento no uso de equipamentos fora do contexto físico das organizações. Porém, também possibilitou que os empregadores passassem a preocupar-se com o monitoramento de seus subordinados[7], fazendo inclusive uso de programas para tal fim.

Diversos destes programas foram postos no mercado nacional e internacional com a finalidade de monitorar o comportamento dos empregados, rastrear suas atividades *online* e analisar sua produtividade (*Hubstaff, Teramind, ActivTrak, Time Doctor, InterGuard, Clockify, Toggl Track, Insightful, Focusme, Veriator, Investiagor*). O programa *Teramind* propõe a detecção de ameaças internas, prevenção contra perda de dados, análise de produtividade e otimização de processos de negócios com tecnologia avançada de análise de comportamento do usuário, anuncia o programa.[8]

Fato a ser notado é que a mesma ferramenta utilizada para o exercício da atividade laboral pode ser usada para o monitoramento do trabalhador.

Vale registrar que o Código de Trabalho de Portugal[9], no seu art. 20 veda o uso de meios de vigilância à distância no local de trabalho, mediante o emprego de equipamento tecnológico, com a finalidade de controlar o desempenho profissional do trabalhador, só considerando tal procedimento como lícito quanto tenha por finalidade resguardar a proteção e segurança de pessoas e bens ou quando particulares exigências inerentes à natureza da atividade o justifiquem.

Acresça-se que o uso associado de som e vídeo possibilita uma intromissão ainda maior nos direitos à privacidade, intimidade e autodeterminação informativa do trabalhador, consoante Parecer 4/2004 do Grupo de Trabalho do art. 29 (GT29) sobre o Tratamento de Dados Pessoais por meio de Videovigilância, de 11 de fevereiro de 2004, orientando

[7] Célio Pereira Oliveira Neto, *Trabalho em ambiente virtual: causas, efeitos e conformação*, 2ª ed., São Paulo, LTr, 2022, p. 295.
[8] https://www.teramind.co/ (30.11.2024).
[9] Portugal, *Código do Trabalho – CT Lei 7/2009*, *in* https://dre.pt/dre/legislacao-consolidada/lei/2009-34546475 (30.11.2024).

a minimização não só da coleta, como também do número de pessoas que tenham acesso aos dados, como corolário da proteção à privacidade e autodeterminação informativa – vedando ainda, de forma expressa, o controle quanto à qualidade e quantidade da atividade laboral.

Visando a autodeterminação informativa, a Organização Internacional do Trabalho (OIT), por meio do Repertório de recomendações práticas sobre proteção de dados pessoais dos trabalhadores, de 1997, estabeleceu, entre outros, a necessidade de prévio conhecimento por parte dos trabalhadores quando estes sofrem controles de medida e vigilância, assim como no que tange às razões que motivam o controle, horas em que o controle será levado a efeito, técnicas utilizadas para tanto e dados a serem coletados, sempre observada a menor invasão à privacidade.

O Parecer 2/2017 GT29, orienta ainda que a vigilância só pode ocorrer por motivo de segurança, saúde e proteção de bens, observada a vedação quanto ao controle oculto, salvo se previsto em legislação nacional ou se existentes fundadas suspeitas de atividades criminosas ou infrações graves, garantindo que os dados sejam tratados para finalidades legítimas, que sejam adequados, necessários e proporcionais, não excessivos para a finalidade, e o empregador seja transparente para com os empregados quanto à utilização e finalidade das tecnologias de monitoramento[10].

No Brasil, por sua vez, o poder diretivo do empregador sofre limitações, de modo que, se o controle for incisivo e contínuo, poderá acarretar o reconhecimento da invasão desmedida da privacidade, em possível violação aos direitos da intimidade e vida privada.[11]

Nesse sentido, quanto à possibilidade de exercício do poder de fiscalização, desde que não avance sobre a intimidade do trabalhador, decisão da 5ª Turma do Tribunal Superior do Trabalho de lavra do Min. Guilherme Caputo Bastos:

> *"o exercício do poder fiscalizatório, realizado de modo impessoal, geral, sem contato físico ou exposição da intimidade, não submete o trabalhador a situação vexatória nem caracteriza humilhação, vez que decorre do poder diretivo do empregador, revelando-se lícita a prática desse ato".*

Significa dizer, que o empregador pode monitorar resultados e metas, mas não tem a faculdade de fiscalizar o trabalhador em si durante todo o curso do trabalho, haja vista que a vigilância à distância pode invadir a esfera da privacidade, e as novas tecnologias combinadas com aplicativos, permitem que o controle por vezes vá além inclusive daquele presencialmente exercido.[12]

Ter consciência dos riscos existentes é fundamental para se tomar decisões sobre que medidas de controle podem ser adotadas pelas equipes de tecnologia da informação e segurança da informação das organizações, tudo com o fim de se atingir o necessário

[10] https://www.uc.pt/protecao-de-dados/suporte/20170608_parecer_2_wp249_gt29 (30.11.2024)
[11] Célio Pereira Oliveira Neto / Ricardo Calcini, «Adequação à LGPD no recrutamento e seleção de candidatos a emprego», *Consultor Jurídico*, 24.09.2020, *in* https://www.conjur.com.br/2020-set-24/pratica-trabalhista-adequacao-lgpd-recrutamento-selecao-candidatos-emprego (30.11.2024).
[12] Célio Pereira Oliveira Neto, *Trabalho em ambiente virtual...*, op. cit.

equilíbrio entre o interesse legítimo dos empregadores, propondo avaliação da proporcionalidade das medidas adotadas nos diferentes cenários antes do início do tratamento, a fim de verificar se de fato este é necessário para atingir uma finalidade legítima, bem como as medidas a serem adotadas para mitigar as restrições do direito à vida privada e à confidencialidade das comunicações, integridade dos dados, controle de acesso ou divulgação não autorizada de informação sensível do empregador.

Pois bem, nas hipóteses de monitoramento à distância, faz-se imperativo o uso do teste de ponderação (*Legitimate Interests Assessment*) como requisito ser cumprido para que o tratamento de dados pessoais seja feito com base no legítimo interesse[13].

Logo, a coleta tem que ter aptidão para cumprir a sua finalidade, inexistindo outro meio menos gravoso com a mesma eficácia, e gerando menos prejuízos do que vantagens, sempre preservado o núcleo essencial do direito preterido.

O Parecer 2/2017 do GT29 apresenta ainda reflexão de que o empregador pode pensar existir uma justificação para implantar pacote de softwares com a capacidade de registrar digitação no teclado, movimento do mouse, capturas de ecrã, registrar as aplicações utilizadas e o tempo de uso, ou mesmo coletar imagens por câmeras web, no entanto, diz o parecer, que o tratamento seria desproporcional, possivelmente sem fundamento jurídico.[14]
Portanto, em respeito à proteção de dados e à privacidade do empregado, se houver monitoramento, é recomendável que o empregador adote os seguintes procedimentos:

i) realizar o teste de ponderação (*Legitimate Interests Assessment*) como requisito ser cumprido para que o tratamento de dados pessoais seja feito com base no legítimo interesse;
ii) implementar rotinas de adequação à LGPD, visando a tutela dos dados dos trabalhadores;
iii) criar política de proteção de dados dos empregados;
iv) informar ao empregado a existência de monitoramento;
v) justificar a necessidade e adequação do monitoramento, sem abuso de poder;
vi) controlar metas e resultados, mas não eventual inatividade dos empregados;
vii) implementar política de teletrabalho, impondo ao empregado ações que preservem sua intimidade e de seus familiares, como por exemplo o uso obrigatório de fundo de tela.

9.3. Conclusão

Considerando a necessidade de se criar uma cultura de proteção de dados no Brasil e elevar o nível de maturidade, ainda incipiente, e acrescendo que o tema aqui tratado não possui regulamentação na seara trabalhista no Brasil, recomenda-se o uso do Direito comparado como paradigma, assim como dos estudos do Grupo de Trabalho do art. 29 (GT29) sobre o Tratamento de Dados Pessoais – claro que mediante as adaptações necessárias.

[13] https://www.uc.pt/site/assets/files/475840/20140409_wp_217_parecer_6_2014_conceito_interesses_legitimos_resp_t_rat_diretiva_95.pdf (30.11.2024)
[14] https://www.uc.pt/protecao-de-dados/suporte/20170608_parecer_2_wp249_gt29 (30.11.2024).

Nessa esteira, importante registrar que, apesar de não existir óbice legal à vigilância à distância do trabalhador no Brasil para avaliação ou medição do desempenho profissional, esta somente é possível desde que não seja desmedida, desproporcional, contínua, com potencial de invadir, assim, a esfera da intimidade, privacidade e proteção de dados.

10. Legislação

Brasil, *Constituição da República Federativa do Brasil*, de 1988
Brasil, *Consolidação das Leis do Trabalho*, Decreto-Lei 5.452 de 1943
Brasil, *Lei 8.078*, de 11 de setembro de 1990
Brasil, *Lei 12.965*, de 23 de abril de 2014
Brasil, *Lei 10.046*, de 10 de janeiro de 2002
Brasil, *Lei 13.709*, de 14 de agosto de 2018
Resoluções e Circulares do Banco Central do Brasil
Resolução nº 4.893, de 26/02/2021, sobre política de segurança cibernética e requisitos para processamento e armazenamento de dados
Circular nº 3.978, de 23/01/2020, estabelece procedimentos e controles internos para prevenção de crimes de lavagem de dinheiro e financiamento ao terrorismo.
Resolução nº 142, de 23/09/2021, sobre prevenção de fraudes em serviços de pagamento
Normas do Setor de Seguros (SUSEP)
Circular SUSEP nº 638/2021, requisitos mínimos de segurança cibernética para proteção de dados pessoais.
Resolução CNSP nº 450/2022, requisitos para credenciamento e funcionamento de sociedades processadoras de ordens de clientes.
Circular SUSEP nº 612/2020, diretrizes para prevenção de lavagem de dinheiro e financiamento ao terrorismo.
Normas e Regulamentações Internacionais
Regulamento Geral de Proteção de Dados (GDPR), artigo 6(1)(f) citado como base legal para prevenção à fraude no contexto europeu.
Pareceres do Grupo de Trabalho do Art. 29 (GT29), parecer 4/2004 sobre videovigilância.
Parecer 2/2017 sobre Legitimate Interests Assessment (LIA),
Organização Internacional do Trabalho (OIT), Repertório de Recomendações Práticas sobre Proteção de Dados Pessoais dos Trabalhadores (1997).
Tratado de Funcionamento da União Europeia (TFUE), citado como base para o trabalho do OLAF (Organismo Europeu de Luta Antifraude).
Resolução Conjunta nº 6, de 23/05/2023, European Data Protection Board, *Article 29 Data Protection Working Party.*
Portugal, *Código do Trabalho – CT Lei 7/2009*

***

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

autentique

Autenticação eletrônica 22/22
Data e horários em GMT -3:00 Sao Paulo
Última atualização em 01 dez 2024 às 21:23
Identificador: 884170fce51a0663d5648e0847fcb2214d625d2453ef2baa9

Página de assinaturas

Martha Leal
479.024.000-25
Signatário

Rafael Reis
007.050.759-74
Signatário

HISTÓRICO

01 dez 2024 18:09:11 — **Rafael Reis** criou este documento. (Empresa: Instituto Nacional de Proteção de Dados, CNPJ: 37.415.768/0001-36, Email: diretoria@inpd.com.br)

01 dez 2024 21:22:58 — **Rafael Almeida Oliveira Reis** *(Email: presidencia@inpd.com.br, CPF: 007.050.759-74)* visualizou este documento por meio do IP 191.177.193.184 localizado em Curitiba - Paraná - Brazil

01 dez 2024 21:23:47 — **Rafael Almeida Oliveira Reis** *(Email: presidencia@inpd.com.br, CPF: 007.050.759-74)* assinou este documento por meio do IP 191.177.193.184 localizado em Curitiba - Paraná - Brazil

01 dez 2024 18:10:04 — **Martha Leal** *(Email: vp@inpd.com.br, CPF: 479.024.000-25)* visualizou este documento por meio do IP 24.103.41.130 localizado em New York - New York - United States

01 dez 2024 18:14:14 — **Martha Leal** *(Email: vp@inpd.com.br, CPF: 479.024.000-25)* assinou este documento por meio do IP 24.103.41.130 localizado em New York - New York - United States

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANEXO XIV – CONTRIBUIÇÕES: MINISTÉRIO PÚBLICO DO TRABALHO (MPT)

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

MINISTÉRIO PÚBLICO DO TRABALHO
Procuradoria Geral do Trabalho
Coordenadoria Nacional de Combate Às Fraudes Nas Relações de Trabalho - Conafret
SAUN Quadra 5, Lote C, Torre A - Asa Norte - Brasília/DF - CEP 70040-250
Tel. (61) 3314-8500 - portal.mpt.mp.br - conafret.assessoria@mpt.mp.br

Processo: PGEA 20.02.0001.0009724/2024-28
Partes: Interessado(a)(s): Coordenadoria Nacional de Combate Às Fraudes Nas Relações de Trabalho - Conafret
Assunto: TEMAS: 01.05.01. - Acompanhamento de Feitos Judiciais/Administrativos
Observação: Processo Autuado

OFÍCIO Nº.8475.2024

À Excelentíssima Senhora
Dra. Lílian Manoela Monteiro Cintra de Melo
Presidente do CNPD

Senhora Presidente,

Cumprimentando-a cordialmente, venho, em resposta ao Ofício de Solicitação de contribuição ao CNPD (GT5), informar que, após o recebimento da solicitação para a apresentação de eventuais contribuições para subsidiar a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade relacionada à temática de dados pessoais para o desenvolvimento econômico, tecnológico e a inovação, esta Coordenadoria Nacional de Combate às Fraudes nas Relações de Trabalho (CONAFRET), considerando a relevância da temática não apenas para o combate às fraudes, mas para todo o Ministério Público do Trabalho, reputou pertinente a consulta às demais Coordenadorias Nacionais Temáticas, para que pudessem apresentar contribuições acerca das respectivas áreas temáticas.

Foi solicitado que as contribuições abordassem os seguintes quesitos:

1) Casos práticos e dados estatísticos que demonstrem a importância do uso e da proteção de dados pessoais para o desenvolvimento econômico, tecnológico e a inovação;
2) Como a LGPD e outras normas aplicáveis, nacionais e internacionais, servem como bússola para que os dados pessoais possam ser utilizados para o desenvolvimento econômico, tecnológico e a inovação, de forma ética, segura e responsável?
3) Quais práticas poderiam ser implementadas para melhorar a proteção de dados e segurança jurídica no tratamento de dados

pessoais para o desenvolvimento econômico, tecnológico e a inovação?

No âmbito da CONAFRET, foi desenvolvido o Projeto Estratégico Nacional Plataformas Digitais, voltado ao combate ao desvirtuamento da relação de emprego por meio da utilização de plataformas digitais.

Superada a fase inicial do Projeto, com ajuizamento de ações judiciais em face das principais plataformas digitais buscando o reconhecimento do vínculo empregatício, a Coordenação Nacional, junto com a Gerência do Projeto, passou a atuar em outros aspectos do trabalho plataformizado, dentre eles a questão relacionada a bloqueios e suspensões realizadas pelas plataformas em desrespeito ao artigo 20 da Lei Geral de Proteção de Dados.

Ao longo dos últimos anos em que o MPT pode se debruçar sobre o trabalho realizado por meio de plataformas digitais, foi possível constatar que as empresas detentoras de tais plataformas realizam um controle das atividades realizadas pelos trabalhadores por meio do algoritmo e, a partir de tais informações, aliadas às notas atribuídas pelos consumidores, o aplicativo pode ofertar bônus ou aplicar sanções, sendo que estas podem abranger suspensões temporárias ou bloqueios permanentes.

Tais penalidades puderam ser constatadas não apenas a partir de estudos e investigações realizadas por este Parquet, mas também a partir de relatos dos próprios trabalhadores, e de associações que os representam. Também foi possível identificar que as plataformas, ao aplicarem tais sanções, não oferecem a possibilidade de apresentação de defesa e, em muitos casos, nem sequer informam o motivo, que só chega a ser descoberto quando do ajuizamento de ações perante o Poder Judiciário.

Verifica-se, portanto, que se trata de decisões prejudiciais aos trabalhadores baseadas unicamente no tratamento automatizado de dados pessoais sem lhes oportunizar a apresentação de defesa ou a possibilidade de solicitar a revisão de tais decisões, em flagrante violação ao artigo 20 da LGPD.

Desta forma, com o objetivo de enfrentar tal situação, sugere-se a implementação de medidas destinadas à conscientização dos trabalhadores titulares de tais dados e à adequação de conduta por parte das empresas proprietárias de plataformas digitais, bem como a fiscalização e responsabilização daquelas que sigam descumprindo o dispositivo.

A Coordenadoria Nacional de Combate ao Trabalho Infantil e de Promoção e Defesa dos Direitos de Crianças e Adolescentes (Coordinfância), por meio de seus Coordenadores Nacionais, Dra. Luísa Carvalho Rodrigues e Dr. André

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

Canuto de Figueiredo Lima, destacou que, em virtude do prazo para manifestação, não foi possível identificar casos práticos ou exemplos da atuação ministerial em defesa dos direitos das crianças e adolescentes que se relacionem à proteção de seus dados em plataformas digitais, mas ressaltou que tem conhecimento de investigações e ações judiciais propostas pelo MPT relacionados ao trabalho infantil via plataformas digitais e que reforça a necessidade de que as plataformas digitais adotem providências para prevenir e combater o trabalho infantil em ambiente digital, que alcança inclusive algumas de suas piores formas, como a exploração sexual de crianças e adolescentes, além de outras violências.

Dentre as providências que entende necessárias, destaca a importância da verificação etária efetiva e confiável, observado a proteção segura de dados sensíveis de pessoas que tenham até 18 anos, sempre de modo a observar o seu melhor interesse, nos termos do art. 14 da LGPD.

Esclarece que a Resolução n. 245/2024 do CONANDA reafirma o art. 227 da Constituição Federal ao indicar deveres de cuidado e responsabilidades das empresas provedoras de produtos e serviços digitais, inclusive quanto à proteção de seus dados.

Por fim, sugere que as discussões quanto à proteção de dados de crianças e adolescentes em situação de trabalho via plataformas digitais sejam travadas sob as diretrizes constitucionais da proteção integral e da prioridade absoluta, uma vez que elas também se destinam a quaisquer empresas ou entidades privadas que lidem com crianças e adolescentes.

A Coordenadoria de Promoção da Igualdade de Oportunidades e Eliminação da Discriminação no Trabalho (Coordigualdade), por meio de sua Coordenadora Nacional, Dra. Danielle Olivares Corrêa, elencou os seguintes casos práticos identificados que demonstram a importância do uso e da proteção de dados pessoais para o desenvolvimento econômico, tecnológico e a inovação:

- Desde 8 de dezembro de 2020, a empresa Uber traz a opção em seu aplicativo, por meio da mudança de preferências, para que motoristas mulheres escolham somente atender passageiras, como iniciativa do projeto interno “Elas na Direção”. A coleta do gênero dos(as) usuários(as) da empresa-aplicativo é indispensável para se atingir as mulheres como público-alvo da política interna a fim de prevenir e eliminar a violência de gênero (https://www.uber.com/br/ptbr/u/elas-na-direcao/);
- A empresa 99 inclui pessoas com deficiência auditiva sendo motoristas parceiros com a disponibilização de adesivos, cabides de retrovisor e encosto de cabeça com as frases “Motorista Deficiente Auditivo”, “Sinalize para conversar comigo” e “Converse comigo por mensagem”. A indicação do tipo de

deficiência permite a efetividade da política interna de inclusão e eliminação de barreiras (https://99app.com/blog/passageiro/respeito-a-diversidade-saiba-o-quea-99-tem-feito/);
- A empresa 99 criou a campanha "dirija como uma garota" para empoderamento feminino para as condutoras, além de atrair mais mulheres a serem motoristas (https://99app.com/blog/passageiro/respeito-a-diversidade-saiba-o-que-a-99-tem-feito/)

Pontuou, ainda, que a proteção da privacidade implica no respeito à autodeterminação informativa dos dados pessoais de trabalhadores e trabalhadoras, que não pode sofrer violação em razão da vigilância digital das plataformas digitais, de modo que a LGPD e demais normas nacionais e internacionais sobre proteção de dados podem ser utilizadas para harmonizar a razão da inteligência artificial, bem como seu gerenciamento de dados e informações, com a hipossuficiência da pessoa trabalhadora, especialmente se esta pertencer a um grupo de alta vulnerabilidade social, a exemplo da população negra, idosos, comunidade LGBTQIAPN+ e pessoas com deficiência. Nessa linha, sinalizou que cabe às plataformas digitais a prevenção de riscos da automação dos processos decisórios quanto a práticas discriminatórias provocadas por algoritmos.

Por fim, sugeriu a implementação das seguintes práticas com vistas a melhorar a proteção de dados e segurança jurídica no tratamento de dados pessoais para o desenvolvimento econômico, tecnológico e a inovação:

- Uso de dados pessoais sensíveis, ainda que sem o consentimento do titular, para promoção de políticas públicas previstas em lei, conforme o art. 11, "b", II da LGPD (Lei nº 13.709/2018);
- Uso de dados pessoais sensíveis para a realização de estudos acadêmicos, vide o art. 11, II, "c" da LGPD (Lei nº 13.709/2018). A coleta de informações de dados sensíveis, a exemplo do gênero, orientação sexual, raça, idade, dentre outros de igual natureza, de trabalhadores(as) em plataformas digitais poderá traçar um perfil da categoria, comprovando a transposição da desigualdade de gênero e raça do trabalho não plataformizado para o trabalho plataformizado;
- Garantia ao titular o direito de acesso às informações sobre o tratamento de seus dados pessoais sensíveis, inclusive em relação à tomada de decisões automatizadas a fim de se coibir suposta discriminação algorítmica em razão da raça, gênero, orientação sexual, idade, dentre outros, considerando o art. 15 do Regulamento 2016/679 do Parlamento Europeu e do Conselho (GDPR) c/c art. 8 da CLT;
- Presunção relativa do não consentimento individual dos trabalhadores, ainda que seja dado sob qualquer forma, individual ou escrito, com ônus da prova para a plataforma digital, para fins de instalação de sistema de monitoramento

por imagem ou vídeo, nos termos do art. 8º e art. 468 da CLT c/c art. 5º, XII, 7º, I, 18, VI, VIII, IX da LGPD (Lei nº 13.709/2018) c/c art. 32 do Regulamento 2016/679 do Parlamento Europeu e do Conselho (GDPR);
- O silêncio ou omissão do trabalhador acerca do monitoramento de dados pessoais, inclusive sensíveis, não poderá constituir um consentimento, o qual deverá ser uma manifestação de vontade livre, específica, informada e inequívoca do titular de dados, conforme o art. 8º da CLT c/c art. 33 do Regulamento 2016/679 do Parlamento Europeu e do Conselho (GDPR);
- Ponderação entre a real necessidade, minimização do uso de dados e proporcionalidade do tratamento para a eventual exigência de biometria para cadastro de trabalhadores(as) em plataformas digitais, nos termos do art. 9.1 e 9.2 do Regulamento 2016/679 do Parlamento Europeu e do Conselho (GDPR) c/ art. 8º da CLT.

A Coordenadoria Nacional de Defesa do Meio Ambiente do Trabalho e da Saúde do Trabalhador e da Trabalhadora (CODEMAT), por meio de suas Coordenadoras Nacionais, Dra. Cirlene Luiza Zimmermann e Dra. Juliane Mombelli, as Coordenadorias Nacionais Temáticas possuem representantes no Núcleo de Proteção de Dados (NPDados) do MPT, coordenado pelo Encarregado de Dados, Dr. José Fernando Ruiz Maturana, com previsão de que sejam debatidas e definidas, nesse espaço, as demandas institucionais relacionadas ao tema.

Destacou que, em contato com a representante da CODEMAT no NPDados, Dra. Eliane Lucina, a Coordenação foi informada de que, até o momento, não haviam sido definidos casos práticos ou estatísticos, nem outras situações que pudessem subsidiar os questionamentos apresentados pelo Conselho Nacional de Proteção de Dados (CNPD), mas destacou que, no dia 12 de dezembro de 2024, será realizado um curso de capacitação intitulado "A Tutela Coletiva do Direito à Proteção de Dados Pessoais no Âmbito das Relações de Trabalho", com o objetivo de aprofundar os estudos e as melhores práticas do MPT sobre o tema.

Sugere, portanto, a manutenção da comunicação com o Conselho Nacional de Proteção de Dados, diante da possibilidade de surgimento de novas demandas a partir dos trabalhos no âmbito do NPDados.

Por fim, a Coordenadoria Nacional de Promoção da Liberdade Sindical e do Diálogo Social (Conalis), por meio de suas Coordenadoras Nacionais, Dra. Viviann Brito Mattos, Dra. Priscila Moreto de Paula e Dra. Lia Magnoler Guedes de Azevedo Rodriguez, apontou para a necessidade de observância rigorosa da Lei Geral de Proteção de Dados (LGPD), particularmente no contexto de bloqueios e outras penalidades impostas a esses trabalhadores, de modo que a proteção adequada dos dados deve garantir o respeito aos princípios fundamentais estabelecidos pela legislação, incluindo a transparência, a finalidade e a

proporcionalidade no tratamento de dados pessoais.

Esclareceu que a liberdade sindical, assegurada pelo art. 8º da Constituição Federal, exige uma atenção especial no tratamento desses dados, de modo a evitar o uso inadequado que possa comprometer direitos fundamentais ou resultar em discriminação ou represálias contra trabalhadores sindicalizados, enfatizando a importância da implementação de mecanismos que garantam o uso responsável dos dados pessoais e sensíveis, protegendo os trabalhadores contra práticas abusivas e assegurando que decisões envolvendo bloqueios ou penalidades sejam baseadas em critérios objetivos, devidamente fundamentados e em conformidade com os direitos assegurados pela LGPD e pela liberdade sindical.

Destacou que a filiação sindical, reconhecida como dado sensível pela LGPD (art. 5º, inciso II), representa um elemento central da organização coletiva dos trabalhadores e que sua proteção é crucial para assegurar a liberdade sindical. Registrou que a afirmação do princípio da liberdade sindical é essencial para a promoção da dignidade da pessoa humana e da justiça social.

Ressalta que o Preâmbulo da Constituição da Organização Internacional do Trabalho (OIT) declara que o modo de produção capitalista produz condições de trabalho que implicam, para a grande maioria das pessoas, miséria e privações, e o sofrimento daí decorrente põe em risco a paz universal e duradoura. Assim, conclui ser urgente buscar melhorar essas condições de trabalho no que se refere ao princípio da liberdade sindical, sendo crucial proteger os dados pessoais dos trabalhadores em matéria sindical com o objetivo de combater a prática de atos antissindicais contra trabalhadores.

Elencou os seguintes atos antissindicais que podem ser praticados caso não haja a proteção dos dados pessoais dos trabalhadores:

a. despedir ou discriminar trabalhadora ou trabalhador em razão de sua filiação a sindicato, participação em greve, assembleia, manifestação ou o engajamento a qualquer atividade sindical;
b. discriminação aos filiados ao sindicato quanto a promoções e aumentos salariais;
c. transferir, deixar de promover ou prejudicar de qualquer forma trabalhadora ou trabalhador em retaliação pela sua atividade sindical;
d. desestimular a filiação sindical;
e. estimular a desfiliação sindical;
f. utilizar meios de comunicação para ataques e ofensas aos sindicatos, seus dirigentes ou aos filiados;
g. impedir trabalhadora ou trabalhador de participar de assembleia legitimamente convocada pela entidade sindical;

h. monitorar, constranger, interferir e manipular, por prepostos ou instrumentos tecnológicos, a livre participação da trabalhadora ou do trabalhador em assembleia legitimamente convocada pela entidade sindical;
i. induzir ou coagir trabalhadora ou trabalhador a desistir ou renunciar a direito objeto de ação judicial proposta por entidade sindical para a defesa de direitos e interesses coletivos ou individuais da categoria;
j. cercear ou dificultar a adesão e o livre exercício do direito de greve;
k. constranger a trabalhadora ou o trabalhador a comparecer ao trabalho, com o objetivo de frustrar ou dificultar o exercício do direito de greve;
l. contratar, fora das hipóteses previstas na lei, trabalhadoras ou trabalhadores para substituir aqueles que aderiram ao movimento paredista legitimamente convocado;
m. implementar prêmio ou qualquer incentivo para incentivar trabalhadora ou trabalhador a não aderir ou participar de greve;
n. subordinar a admissão ou a preservação do emprego a não filiação a entidade sindical;
o. conceder tratamento discriminatório em virtude de filiação ou atividade sindical;
p. financiar, facilitar, promover a criação de sindicato, com o único intuito de atender aos interesses do empregador ou do sindicato patronal;
q. sabotar ou proibir campanha de filiação sindical dentro dos locais de trabalho;
r. estimular, sugerir, auxiliar e induzir a trabalhadora ou o trabalhador a apresentar cartas de oposição ao desconto da contribuição instituída em negociação coletiva;
s. restringir ou dificultar o recebimento das mensalidades sindicais e demais contribuições destinadas ao financiamento do sindicato profissional estabelecidas na lei, nos instrumentos normativos ou no estatuto do sindicato.

Destacou que a LGPD orienta o uso de dados para atender às necessidades econômicas e tecnológicas sem comprometer direitos fundamentais, de modo que, no contexto sindical, a LGPD promove um ambiente seguro para a filiação e a atuação coletiva, viabilizando tanto o desenvolvimento de novas plataformas tecnológicas para gestão sindical quanto a integração segura dos trabalhadores em sistemas econômicos inovadores.

Reputou imprescindível a implementação de medidas visando proteger os dados sindicais dos trabalhadores, buscando um equilíbrio entre as inovações tecnológicas das plataformas digitais e a proteção dos direitos fundamentais dos trabalhadores.

Por fim, entendeu que as práticas a serem implementadas para melhorar a proteção de dados e segurança jurídica no tratamento de dados pessoais sindicais dos trabalhadores seriam mais efetivas com a oportunidade de participação democrática da classe trabalhadora nessa construção, sugerindo que as Centrais

Sindicais e demais organizações de trabalhadores pudessem participar dessa construção.

Sendo o que havia para o momento, renovo os votos de elevada estima e consideração e coloco-me à disposição para os esclarecimentos que se façam necessários.

Atenciosamente,

São Paulo/SP, data da assinatura eletrônica

(assinado eletronicamente)
RENAN BERNARDI KALIL
PROCURADOR DO TRABALHO
COORDENADOR NACIONAL DA CONAFRET

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANEXO XV – CONTRIBUIÇÕES: MOVIMENTO BRASIL COMPETITIVO (MBC)

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

Brasília, 29 de novembro de 2024.

A Sua Senhoria o Senhor
Rony Vainzof
Conselheiro Titular e Coordenador do GT5
Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

Assunto: Contribuições do MBC ao GT5 do CNPD.

Prezado Senhor Rony Vainzof,

O Movimento Brasil Competitivo (MBC) é uma organização da sociedade civil, apartidária, que conecta os setores público e privado para promover a competitividade nacional, fortalecer a capacidade de investimento do Estado e aprimorar os serviços públicos essenciais oferecidos à população. Para o MBC, a transformação digital é essencial, e defendemos uma política de Estado que valorize a economia digital, impulsionando a melhoria do ambiente de negócios e promovendo um crescimento econômico mais inclusivo e sustentável.

Em atenção à solicitação de contribuições para o Grupo de Trabalho dedicado à temática de dados pessoais para o desenvolvimento econômico, tecnológico e a inovação (GT5), conforme Portaria CNPD nº 05/24, o MBC apresenta abaixo suas considerações acerca dos quesitos propostos.

---

1. Casos práticos e dados estatísticos

O MBC entende que as leis de proteção de dados pessoais, como a Lei Geral de Proteção de Dados Pessoais (LGPD), têm como objetivo principal assegurar o tratamento adequado das informações, garantindo a privacidade e a segurança dos titulares. Assim, destacamos:

- **Exemplo prático**: utilização de softwares para a gestão de consentimento em empresas, como sistemas que automatizam a autorização para uso de imagens de colaboradores em eventos corporativos. Esta prática é um exemplo de como é possível alinhar conformidade legal com a promoção da transparência e do controle por parte dos titulares.
- **Dados estatísticos**: ressaltamos a necessidade de estudos que evidenciem o impacto positivo do uso responsável de dados no crescimento econômico e no fomento à inovação, reforçando a percepção de que legislações protetivas podem ser aliadas do desenvolvimento.

2. LGPD e outras normas como bússola para o desenvolvimento

Concordamos que a LGPD, juntamente com resoluções, notas técnicas e Guias Orientativos emitidos pela Autoridade Nacional de Proteção de Dados (ANPD), constituem uma base normativa essencial para garantir:

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

MBC

- **Segurança e previsibilidade jurídica**: essas normas orientam empresas e organizações a utilizarem dados pessoais de maneira ética, segura e em conformidade legal.
- **Inovação com responsabilidade**: ao criar um ambiente regulatório robusto, possibilitam que empresas explorem o potencial dos dados pessoais, promovendo soluções tecnológicas inovadoras sem comprometer os direitos dos titulares.

Nesse contexto, reforçamos a importância de uma regulação harmônica, que equilibre o fomento ao desenvolvimento econômico com a preservação da privacidade e segurança dos dados pessoais.

3. Práticas para aprimorar a proteção de dados

Neste momento, o MBC não apresentará contribuições específicas para este quesito. Permanecemos, no entanto, à disposição para colaborar em futuras discussões que envolvam soluções e estratégias para o aprimoramento da proteção de dados pessoais no Brasil.

Agradecemos a oportunidade de contribuir com este relevante processo e reiteramos nosso compromisso em colaborar para que a Política Nacional de Proteção de Dados Pessoais e da Privacidade (PNPD) reflita as necessidades do setor produtivo e promova o desenvolvimento econômico, tecnológico e a inovação de maneira ética e sustentável.

Permanecemos à disposição para esta ou futuras discussões que possam enriquecer os trabalhos do GT5.

Atenciosamente,

Tatiana Ribeiro

Tatiana Ribeiro
Diretora-Executiva do Movimento Brasil Competitivo

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANEXO XVI – CONTRIBUIÇÕES: UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO (URFPE)

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

Contribuição ao Conselho Nacional de Proteção de Dados (GT5)

Prezados membros da CAPD,

Abaixo, listo contribuições de acordo com os quesitos solicitados em ofício. Para isso, me atenho ao contexto dos estudos que o nosso grupo de pesquisa realiza sobre plataformas de software e seus impactos em crianças e adolescentes.

1) Casos práticos e dados estatísticos que demonstrem a importância do uso e da proteção de dados pessoais para o desenvolvimento econômico, tecnológico e a inovação.

As pesquisas conduzidas pelo nosso grupo nos últimos anos abordam a importância da proteção de dados, especialmente para crianças e adolescentes, no contexto do desenvolvimento de plataformas digitais (ex.: de mídias sociais e jogos). Embora não apresentemos dados estatísticos que correlacionem diretamente a proteção de dados com o desenvolvimento econômico, tecnológico e a inovação, considerando nossa ênfase em métodos qualitativos ou de mapeamentos sistemáticos na literatura formal e cinza (ex.: relatórios de instituições do terceiro setor, notícias de portais e imprensa nacional e internacional de relevância, etc.), os nossos artigos destacam como a coleta e o uso responsável de dados podem fomentar a confiança dos usuários, impulsionar a inovação ética ou responsável e garantir a sustentabilidade a longo prazo das plataformas, que entendemos serem elementos fundamentais para o desenvolvimento em todas as áreas. Detalhamos estes aspectos abaixo:

- A **confiança** dos usuários é essencial para o desenvolvimento econômico de plataformas digitais e está ligada ao poder de referência que possuem (status ou reputação). Plataformas que demonstram respeito pela privacidade e proteção de dados tendem a atrair mais usuários e, consequentemente, gerar mais receita. A falta de transparência (por exemplo, na moderação de conteúdo ou na forma como os dados são tratados) e o uso de dados para manipulação, por outro lado, podem gerar desconfiança e prejudicar a reputação da plataforma, impactando negativamente seu crescimento.
- O **uso responsável** de dados pode impulsionar a inovação ética. Quando empresas de dados ou tecnologia priorizam a privacidade desde a concepção de seus produtos (conceito de *Privacy by Design / Default* presente nas legislações do tipo), elas são incentivadas a buscar soluções inovadoras que protejam os dados dos usuários e, ao mesmo tempo, permitam uma experiência com o sérvio que seja de qualidade. O desenvolvimento de tecnologias como a Inteligência Artificial depende da disponibilidade de dados, mas essa coleta e uso devem ser feitos de forma ética e transparente para garantir a confiança do público e evitar consequências negativas.
- A **sustentabilidade** a longo prazo destas plataformas está baseada na capacidade que elas têm de se adaptar às demandas e expectativas da sociedade, incluindo a crescente preocupação com a privacidade (fruto de movimentos graduais de letramento digital ou de notícias que descortinam brechas de privacidade ou falhas neste processo). Empresas de tecnologia que ignoram a proteção de dados podem enfrentar problemas legais, além de perda de usuários (um ativo essencial para os seus ecossistemas de

software) e danos à sua reputação (como dito acima, o seu poder de referência), comprometendo sua viabilidade futura. Investir em práticas de proteção de dados pode, desta forma, ser um investimento na sustentabilidade dos seus modelos de negócio.

Como casos práticos abordados em nossos trabalhos, para fins de ilustração sobre a importância da proteção de dados, temos:

- O caso da plataforma de jogos **Roblox**, que demonstra como a exploração de dados de crianças pode ter consequências negativas. A plataforma foi acusada de incentivar o trabalho infantil e criar expectativas irreais de ganhos financeiros, utilizando a criatividade e o trabalho de crianças para gerar lucro sem oferecer as devidas proteções.
- Em plataformas de mídia social como **Instagram e TikTok**, há a presença constante de padrões manipulativos e enganosos de design (o que chamávamos de *dark patterns*, termo racializado que vem sendo substituído por *deceptive patterns*[1]), como a rolagem infinita e notificações constantes demonstra como o projeto das suas funcionalidades pode ser usado para influenciar negativamente o comportamento dos usuários e mantê-los engajados por mais tempo, muitas vezes em detrimento do seu bem-estar. A regulamentação dessas práticas, como a Lei de Serviços Digitais (DSA) na União Europeia, busca proteger os usuários e garantir que as plataformas atuem de forma mais transparente e responsável. A coleta massiva de dados e o uso destes padrões contribuem para o modelo orientado à atenção destas plataformas, que pode ter consequências negativas como a proliferação de desinformação e maior polarização.
- **Robôs sociais ou brinquedos inteligentes** como a *Hello Barbie* coletam dados de voz das crianças e os envia para servidores da empresa, algo que foi alvo de críticas por questões de privacidade e segurança. A coleta de dados sensíveis de crianças sem o devido cuidado pode ter consequências negativas para o seu desenvolvimento e bem-estar. O uso de dados de crianças nestes dispositivos deve ser feito com o consentimento informado dos responsáveis, que devem ter acesso às informações coletadas e poder controlá-las (inclusive, de forma simples, sem padrões de manipulação como Interferência Visual, que cria "fricção" nas interfaces para dificultar esta gestão.
- O conceito de **design justo** (*Fair Patterns* ou *Bright Patterns*), que propõe soluções para combater os padrões antiéticos acima e criar plataformas que respeitem a autonomia e o bem-estar dos usuários. A implementação de padrões como "Informação Adequada" e "Ação Livre", por exemplo, pode ajudar os usuários a entender as consequências de suas ações em termos de proteção de dados e decisões mais conscientes sobre como são usados. Isso é feito com um padrão ético denominado *Honest Default*, que propõe uma configuração básica voltada à proteção dos usuários – algo que não ocorre no TikTok, onde contas são abertas por padrão, mas que é a premissa do "modo adolescente" do Instagram a ser lançado no Brasil em janeiro de 2025.

Desta forma, os artigos do grupo reforçam a premissa de que a proteção de dados pessoais é chave para o desenvolvimento de plataformas digitais éticas e inovadoras. A falta de dados estatísticos específicos nos nossos estudos não invalida essa argumentação, considerando que os casos práticos e a análise do impacto da coleta e uso de dados demonstram a importância da proteção de dados para a construção de um ambiente digital mais justo, confiável e responsável.

[1] Deceptive Patterns - https://www.deceptive.design/types

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

2) Como a LGPD e outras normas aplicáveis, nacionais e internacionais, servem como bússola para que os dados pessoais possam ser utilizados para o desenvolvimento econômico, tecnológico e a inovação, de forma ética, segura e responsável?

A LGPD e outros dispositivos, como COPPA, DSA e GDPR, são essenciais para orientação do uso de dados pessoais para o desenvolvimento econômico, tecnológico e inovação no contexto de plataformas de software (sejam elas as de mídias sociais, *games* ou mesmo *e-commerce*), garantindo que o uso seja ético e segura. Abordamos estes normativos, a partir dos nossos estudos, a seguir:

- **LGPD:** aqui, reconhecemos que a nossa lei de proteção de dados estabelece princípios básicos para o tratamento de dados pessoais, como finalidade, necessidade e transparência. São princípios que atuam como diretrizes para as empresas de software (ex.: ByteDance, Meta, Google, empresas menores que desenvolvem jogos ou aplicativos focados em crianças) que coletam e utilizam dados, garantindo que estas atividades respeitem os direitos dos titulares dos dados. A LGPD também prevê direitos aos titulares dos dados, como o direito de acesso, retificação, exclusão e oposição ao tratamento de seus dados. Isso garante que os indivíduos tenham controle sobre seus próprios dados e possam se opor a usos que considerem inadequados ou abusivos. Em nossos estudos, reforçamos que a LGPD se aplica a todos os tipos de dados pessoais, incluindo aqueles coletados por plataformas digitais, jogos eletrônicos e brinquedos inteligentes. Isso significa que as empresas que desenvolvem e operam essas tecnologias devem se adequar à lei, garantindo a proteção dos dados das crianças e adolescentes, que são especialmente vulneráveis nesse contexto.
- **Regulamento Geral de Proteção de Dados (GDPR) da União Europeia:** de forma análoga à LGPD, este regulamento reforça um consenso global sobre a importância da proteção de dados. Como o GDPR inspirou a elaboração da lei de proteção de dados nacional, temos uma convergência entre legislações que facilita a cooperação entre países e empresas, criando um ambiente mais frutífero para o desenvolvimento tecnológico.
- **Marco Civil da Internet** no Brasil e a **Convenção sobre os Direitos da Criança (CDC)** das Nações Unidas reforçam a importância da proteção de dados no contexto da internet e do desenvolvimento infantil, complementando a LGPD e criando um arcabouço legal mais robusto.
- Por fim, reforçamos a importância da recente definição da **Lei de Serviços Digitais (DSA)** da União Europeia, que visa combater práticas abusivas de plataformas digitais, como o uso de padrões de design manipulativo e enganoso que impede o acesso fácil às configurações de privacidade (via padrões como *Interferência Visual* e *Obstrução*, aumentado o número de ações até um serviço que coleta dados excessivamente ser cancelado por um usuário – no caso de um adolescente que não quisesse ter os seus dados usados para treinamento de IAs da Meta, o total de etapas para impedimento deste uso era oito), contribuindo para um ambiente digital transparente e responsável.

Em relação à inovação, a proteção de dados também atua com um importante fator de impulsionamento, inclusive. Quando empresas de software são obrigadas a proteger os dados dos usuários em suas plataformas, elas precisam buscar soluções mais criativas e inovadoras que respeitem a privacidade e, ao mesmo tempo, atendam às suas necessidades de negócio.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

Aqui, o conceito de *Privacy by Design* encoraja a inclusão da proteção de dados desde a concepção de produtos e serviços, levando à criação de tecnologias mais seguras e confiáveis. Por exemplo, a ação judicial contra a Roblox por suposta exploração de dados e trabalho infantil demonstra como a legislação de proteção de dados pode ser utilizada para responsabilizar empresas que não atuam de forma responsável, sem primar pelo melhor interesse da criança. Já a implementação de medidas de segurança e privacidade em plataformas como TikTok em resposta à pressão de órgãos reguladores e da sociedade civil demonstrou neste ano o impacto positivo da legislação na proteção dos usuários. Por fim, como temos investigado, as ferramentas ou funcionalidades de mediação parental nas plataformas precisam se somar às campanhas de educação digital, sendo exemplos de como a legislação pode incentivar a criação de soluções que empoderam os usuários e garantem o uso responsável da tecnologia. Assim, entendemos que a proteção de dados não é um entrave, mas sim um catalisador para o progresso, abrindo caminho para um futuro digital mais ético e justo (*Design Justice*).

3) Quais práticas poderiam ser implementadas para melhorar a proteção de dados e segurança jurídica no tratamento de dados pessoais para o desenvolvimento econômico, tecnológico e a inovação?

Com base nos nossos estudos (aqueles com foco em criança estão listados aqui), derivamos as práticas abaixo, que podem ser implementadas para aperfeiçoar a proteção de dados no contexto tecnológico, especialmente quando se trata de usuários jovens. Reforçamos a a necessidade de uma abordagem multifacetada que envolva as empresas de tecnologia, legisladores, responsáveis e educadores – além das próprias crianças no debate.

1. **Design Ético e Centrado no Usuário:** plataformas devem ser impedidas de adotar padrões enganosos e manipulativos de design, que visam controlar a tomada de decisão e que retiram a autonomia – e por tabela o bem-estar – de crianças e adolescentes. É fundamental priorizar a transparência, o controle por este grupo e a navegação intuitiva e simples, permitindo que estes usuários tomem decisões conscientes e informadas.
2. **Implementação de *Fair Design Patterns***: este conceito recente, de 2023, envolve inúmeros "padrões iluminadores de design", que promovem uma experiência mais ética e respeitosa, priorizando a autonomia do usuário, a transparência na coleta e no uso de dados, e a facilidade de acesso a configurações de privacidade. Seria a antítese dos padrões obscuros de design que assolam inúmeras tecnologias.
3. **Design Adequado à Idade:** as plataformas devem considerar as necessidades e vulnerabilidades de diferentes faixas etárias, especialmente crianças e adolescentes, oferecendo interfaces e funcionalidades adequadas à sua capacidade de compreensão e discernimento. Ao mesmo tempo, não devem usar este artifício para promover padrões excessivamente lúdicos, como *Fofura* (*Cuteness*), que busca criar vínculos emocionais com a criança para fins de manipulação e miopia de dados.
4. **Empoderamento dos Usuários e Educação Digital:** campanhas e sites ligados às plataformas que tragam conscientização sobre direitos digitais e a importância da proteção de dados são essenciais para empoderar crianças e adolescentes, tornando-os mais conscientes dos riscos e capazes de se protegerem. Literacia digital é essencial.
5. **Educação Digital nas Escolas:** com o avanço ou talvez o total espalhamento de tecnologias como Google Sala de Aula, sistemas de reconhecimento facial e até os

próprios LLMs, precisamos assegurar a inclusão da educação digital no currículo escolar, desde a infância. Assim, formamos cidadãos digitais mais críticos e responsáveis. No mais, é uma forma de educadores também poderem abordar conceitos básicos sobre privacidade, segurança online e o uso ético da tecnologia por crianças e adolescentes, que usam mídias sociais para socialização ou *chatbots* para criar projetos escolares.

6. **Ferramentas de Controle Parental:** é necessário disseminar funcionalidades de mediação parental como módulos nas plataformas. No entanto, eles precisam ser fáceis de usar para que os responsáveis acompanhem e limitem o acesso de crianças e adolescentes a conteúdos e plataformas online. E, para fins de privacidade, algo preconizado pela LGPD, cabe refletir sobre se controle parental é adequado ou é uma abordagem intervencionista, que pode promover vigilância dos jovens.
7. **Políticas de Privacidade Claras e Acessíveis:** as empresas de tecnologia devem adotar políticas de privacidade que sejam claras e fáceis de compreender por todos os usuários, independentemente de idade ou nível de conhecimento técnico (ou seja, reforçarmos aqui, assim como em artigos, a ideia de um olhar interseccional – de que infância estamos falando?). A linguagem utilizada deve ser simples e objetiva, evitando jargões técnicos ou termos jurídicos que sejam muito complexos. Além disso, precisam estar no idioma do usuário.
8. **Relatórios de Transparência Detalhados:** empresas como ByteDance, responsável pelo TikTok, devem publicar relatórios de transparência detalhados sobre suas práticas de coleta e uso de dados, incluindo informações sobre os tipos de dados coletados, a finalidade da coleta, os mecanismos de segurança utilizados e os direitos dos usuários. A disponibilização dessas informações de forma acessível e transparente contribui para a construção de um ambiente de confiança e responsabilização.
9. **Investimento em Pesquisa:** é fundamental incentivar o investimento em pesquisa e desenvolvimento de novas tecnologias e soluções que promovam a privacidade e a segurança dos dados, como técnicas de anonimização e criptografia (ideia recente de *client-side scanning*, passível de muitas críticas). O avanço tecnológico deve caminhar lado a lado com a proteção dos direitos dos usuários. Aqui, reforçamos, na ótica da academia, a colaboração entre pesquisadores, indústria e governo para impulsionar a inovação em privacidade e garantir que as novas tecnologias sejam desenvolvidas e utilizadas de forma ética e responsável. A troca de conhecimentos e experiências entre esses atores garante a criação de soluções adequadas às necessidades de grupos específicos como crianças e adolescentes.

Reforçamos que a implementação das práticas acima em conjunto com um esforço contínuo de educação e conscientização contribuirá para a construção de um ambiente digital mais seguro, onde a proteção de dados pessoais seja vista como uma prioridade e a inovação tecnológica se dê sem comprometer os direitos e o bem-estar dos usuários.

Finalizo este opinativo reforçando o interesse do nosso grupo de pesquisa em contribuir de forma regular com este GT, caso seja de interesse do CNPD. Os estudos que conduzimos são de natureza qualitativa, com uma perspectiva que valoriza a subjetividade deste cenário (sem um retrato puramente numérico). Minha proposta é de aportar soluções (sejam elas de software ou mais conceituais) para os trabalhos em curso no cenário de crianças e plataformas.

Nos últimos anos, vimos conduzindo estudos neste contexto. São pesquisas ligadas a temas como padrões de design para manipulação de crianças pelas plataformas, ferramentas de controle parental em apps usados por crianças e requisitos legais de software para

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

conformidade das plataformas com o bem-estar da criança. Todas elas são atravessadas por questões de privacidade, segurança e proteção de dados, sem exceção. Entre 2022 e 2024, oito artigos de conferência e periódicos retratam nossos achados.

Ats,

George Augusto Valença Santos

Professor Associado do Departamento de Computação da UFRPE

gov.br Documento assinado digitalmente
GEORGE AUGUSTO VALENCA SANTOS
Data: 01/12/2024 17:48:20-0300
Verifique em https://validar.iti.gov.br

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANEXO XVII – CONTRIBUIÇÕES: INSTITUTO ALANA

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

São Paulo, 27 de janeiro de 2024

Ref: Solicitação de contribuição ao CNPD (GT 5)

Prezado Sr. Rony Vainzof, coordenador do GT5 do CNPD,

Em resposta ao ofício recebido em 14/11/2024, o **Instituto Alana** vem apresentar referências potencialmente interessantes para as discussões acerca do uso de dados pessoais para o desenvolvimento econômico, tecnológico e a inovação, com enfoque nos dados pessoais de crianças e adolescentes. Desde logo, o Instituto Alana coloca-se à plena disposição para aprofundar o diálogo sobre essas iniciativas e as suas possíveis articulações com os trabalhos deste GT.

- Nota Técnica do Instituto Alana sobre o PL 2338 - Contribuições do Instituto Alana ao substitutivo preliminar do PL 2.338/2023, com considerações sobre o uso de Inteligência Artificial para a promoção com prioridade absoluta dos direitos e do melhor interesse de crianças e adolescentes no Brasil.
- A Escola no Mundo Digital - Dados e Direitos de Estudantes - Guia elaborado em conjunto por Educadigital, Intervozes e Instituto Alana sobre a importância da proteção de dados pessoais estudantis e de modelos alternativos para uma educação livre de exploração comercial e respeitosa à privacidade e segurança de crianças e adolescentes.
- Em anexo, enviamos a contribuição que o Instituto Alana submeteu ao processo de tomada de subsídios acerca do tratamento dos dados pessoais de crianças e adolescentes, que esteve aberto para consulta pública no site da ANPD, entre 17 de junho a 16 de julho de 2024.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

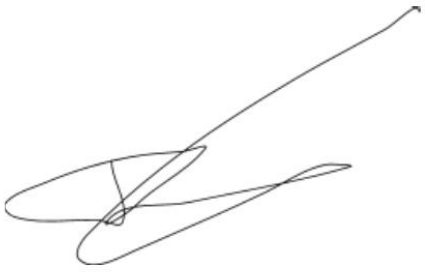
GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

alana

Sendo o que cumpria para o momento, o Instituto Alana segue à disposição deste GT para contribuir com todo o necessário.

Cordialmente,

João Francisco de Aguiar Coelho
Advogado do programa Criança e Consumo



Renato Godoy de Toledo
Gerente de Relações Governamentais

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANEXO XVIII – ESTUDO DE CASO: INTELIGÊNCIA ARTIFICIAL

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ESTUDO DE CASO: INTELIGÊNCIA ARTIFICIAL

Conselheiro da ANPD: Rony Vainzof[6]

SUMÁRIO

[6] Conselheiro titular do CNPD. O trabalho contou com o apoio dos pesquisadores Verônica Barros e Mateus Lamonica.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

1. INTRODUÇÃO

A Inteligência Artificial (IA) é tecnologia condicionante para o desenvolvimento econômico, social e digital de qualquer nação no século XXI. Ela nos permite explorar níveis de conhecimento há poucos anos inimagináveis, abrindo margem para novas descobertas e contribuindo com a possível solução de grandes desafios para a humanidade na atualidade, como o tratamento de doenças graves e mitigação de surtos pandêmicos, alterações climáticas, gestão de riscos financeiros, prevenção a catástrofes naturais e a ilícitos cibernéticos.

Sua capacidade de analisar grandes volumes de dados, incluindo dados pessoais, identificar padrões complexos e executar tarefas com alta precisão está revolucionando a sociedade e a economia, em seus mais diversos setores, desde saúde, serviços financeiros, marketing, alcançando a indústria e chegando até a educação.

Ou seja, a Inteligência Artificial não é apenas uma ferramenta tecnológica, mas um vetor estratégico para o progresso econômico, a evolução tecnológica e a promoção da inovação em escala global. Sua adoção responsável e estratégica é essencial para maximizar seus benefícios e garantir um impacto positivo e sustentável na sociedade.

Assim, o presente Estudo de Caso pretende demonstrar a importância da proteção dos dados pessoais para o desenvolvimento econômico, tecnológico e a inovação quando sistemas de IA envolverem atividades de tratamento de dados pessoais.

2. A IMPORTÂNCIA DO USO E DA PROTEÇÃO DE DADOS PESSOAIS PARA DESENVOLVER E APLICAR A IA, EM PROL DO CRESCIMENTO ECONÔMICO, TECNOLÓGICO E DA INOVAÇÃO RESPONSÁVEL.

Sistemas de IA nem sempre dependem do tratamento de dados pessoais, contudo, é certo que muitos utilizam grandes volumes dessas informações para oferecer soluções mais eficientes e precisas, trazendo benefícios significativos à sociedade, às organizações e ao país.

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

A eficácia dos sistemas de IA depende amplamente da disponibilidade e do tratamento de dados[7] e a relação entre IA e desenvolvimento econômico está fundamentalmente ligada ao uso de dados pessoais para aprimorar processos de tomada de decisão e otimizar operações empresariais.
Importante lembrar e ponderar que modelos de IA possuem eficácia limitada a depender da qualidade dos dados utilizados em seu treinamento. Normalmente, o conjunto de treinamento, no estado original de sua coleta, pode não ser apropriado para o aprendizado de máquina. Portanto, são aplicadas operações para seleção dos dados, remoção de erros e ruídos, equilíbrio da diversidade dos dados (balanceamento), adequação do formato das informações, entre outros. Tais operações compõem a etapa de pré-processamento de um sistema de IA e seu resultado influencia diretamente a qualidade do modelo gerado. Isso porque dados incorretos, mal formatados, ou enviesados tendem a gerar modelos questionáveis.

Abaixo, seguem alguns casos práticos que demonstram finalidades existentes com o uso de sistemas de IA:

- Autenticação de identidade: valida acessos com base em padrões de comportamento e biometria;
- Detecção de identidade falsa: identifica tentativas de fraude ao cruzar dados fornecidos com bases confiáveis;
- Detecção de fraudes: identifica transações atípicas com base em inúmeros dados comportamentais;
- Detecção de lavagem de dinheiro: identifica transações incomuns em operações financeiras;
- Segurança cibernética: monitora e responde a ameaças digitais com análise comportamental;
- Proteção ao crédito: avalia histórico financeiro e comportamento para concessão de crédito;
- Gestão financeira pessoal: monitora gastos e receitas para sugerir economias e investimentos;
- Diagnóstico personalizado: usa históricos médicos, sintomas relatados e dados de exames para prever doenças;
- Prevenção de doenças: utiliza hábitos de saúde para sugestões de melhorias;
- Monitoramento de saúde: dispositivos vestíveis que analisam dados em tempo real para detectar irregularidades;

[7] AGRAWAL, Ajay; GANS, Joshua; GOLDFARB, Avi. *The simple economics of machine intelligence. Harvard Business Review*, v. 17, n. 1, p. 2-5, 2016. Disponível em: https://scholar.google.com/scholar_url?url=https://chemistry.beloit.edu/classes/nanotech/prediction.pdf&hl=pt-BR&sa=T&oi=gsr-r-ggp&ct=res&cd=0&d=14694779099147844352&ei=dylSZ9vfBI6_y9YPncPB6Q8&scisig=AFWwaebUNFRg89GHrBVzJtx7TatB.

- Educação personalizada: adapta conteúdos educacionais de acordo com o progresso e dificuldades do aluno;
- Assistentes virtuais: personalizam interações e executam tarefas com base em preferências e histórico do usuário;
- E-commerce: oferece produtos e promoções personalizadas com base no comportamento de compra;
- Publicidade e marketing: segmentam campanhas e ajustam mensagens com base no perfil do consumidor;
- Recomendações de Streaming: sugerem filmes, músicas e vídeos analisando padrões de consumo.
- Personalização de *feed*: mostra conteúdos relevantes de acordo com engajamento e preferências;
- Remoção de conteúdos prejudiciais: sinaliza automaticamente postagens que contenham discurso de ódio ou incitação à violência e, em alguns casos, são removidas após análise em redes sociais. Alguns conteúdos nocivos podem ser ocultados automaticamente antes mesmo de serem vistos por outros usuários;
- Verificação de fatos: compartilha notícias com bancos de dados de verificadores para alertar o usuário sobre possíveis informações falsas;
- Categorização de preferências: cria experiências de navegação específicas para cada cliente;
- Navegação e transporte: otimizam rotas e preveem tráfego com base em dados de localização;
- Caronas compartilhadas: combinam passageiros com trajetos semelhantes para economia e eficiência;
- Seleção de candidatos: analisa currículos e comportamentos para identificar talentos;
- Engajamento de funcionários: monitora o bem-estar dos colaboradores com sugestões de melhorias;
- Planejamento de carreira: sugere treinamentos e oportunidades de crescimento profissional;
- Planejamento de viagens: elabora itinerários baseados nas preferências do usuário;
- Personalização em hotéis: ajusta serviços e recomendações de atividades com base no perfil do hóspede.

Nessa linha de ideias, segundo o relatório de 2024 do *Stanford Institute for Human-Centered Artificial Intelligence (*HAI)[8], os casos de uso de IA mais comumente adotados, por função, entre as empresas pesquisadas em 2023 foram: (i) automação de *contact center* (26%); (ii) personalização (23%), (iii) aquisição de clientes (22%) e (iv) melhorias de produtos baseadas em IA (22%). O gráfico abaixo mostra a proporção de empresas pesquisadas que usam IA para funções específicas, muitas delas relacionadas a tratamento de dados pessoais.

8 *STANFORD INSTITUTE FOR HUMAN-CENTERED ARTIFICIAL INTELLIGENCE (HAI). AI Index Report 2024*, p. 47. Disponível em: https://aiindex.stanford.edu/wp-content/uploads/2024/05/HAI_AI-Index-Report-2024.pdf.

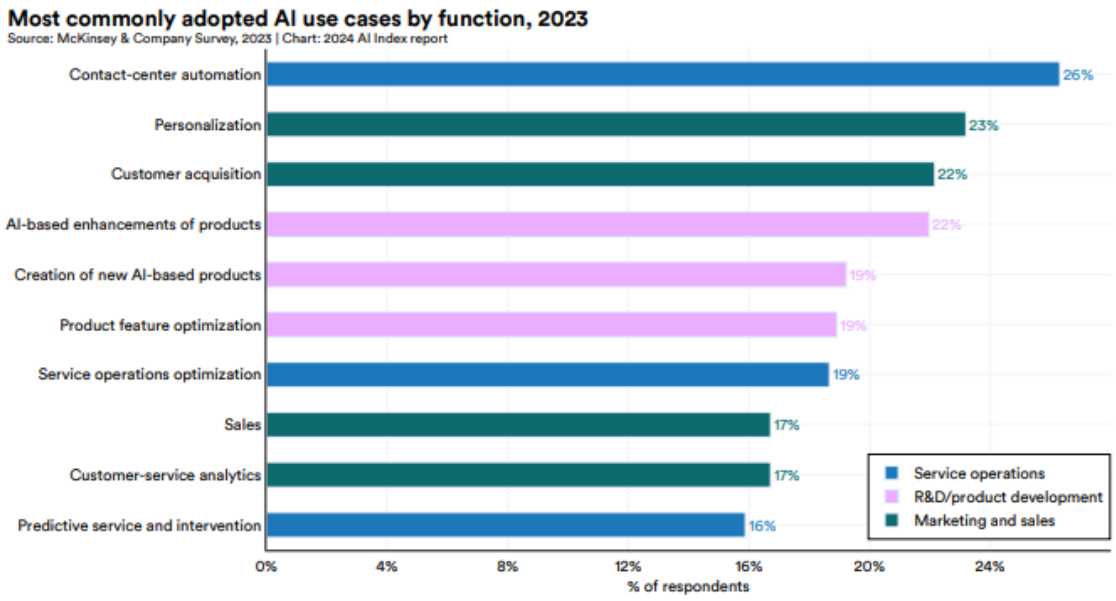


Figure 4.4.2

Em todos os setores, as tecnologias de IA mais incorporadas foram compreensão de texto NL (30%), automação de processos robóticos (30%) e agentes virtuais (30%). O gráfico abaixo demonstra, por setor, os usos de sistemas de IA que mais envolvem dados pessoais:

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

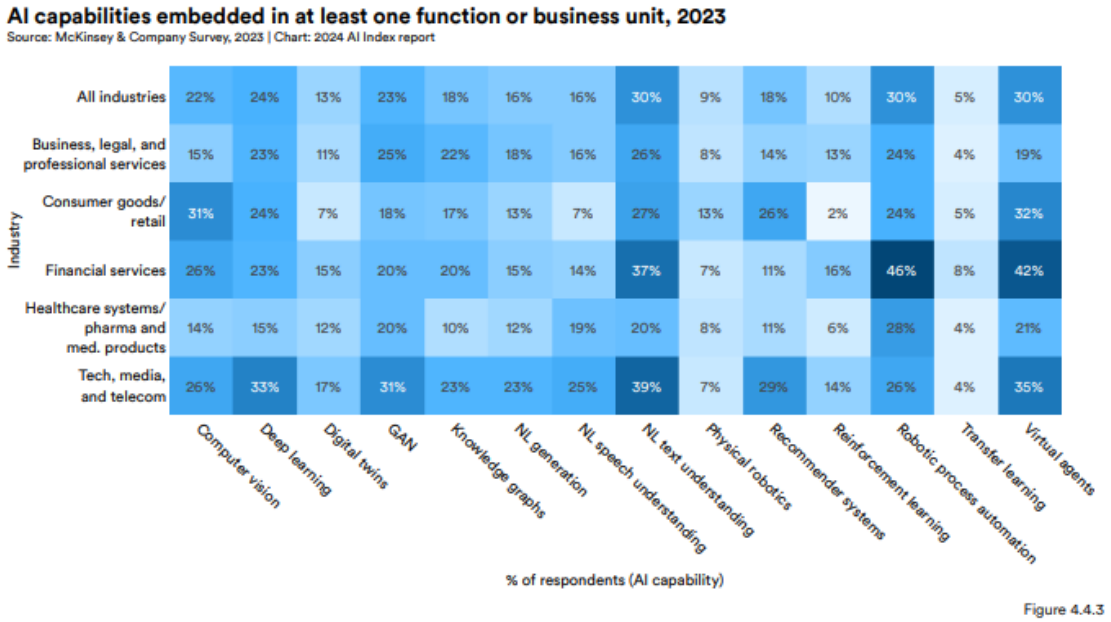


Figure 4.4.3

No contexto brasileiro, a própria proposta do Plano Brasileiro de Inteligência Artificial (PBIA), elaborada pelo Ministério da Ciência, Tecnologia e Inovação – MCTI[9] - a pedido do Presidente da República que expressamente consagra a inteligência artificial como "uma ferramenta capaz de alavancar o desenvolvimento social e econômico do Brasil" demonstra a importância do uso dos dados pessoais para atingir a sua finalidade em diversas passagens, conforme abaixo detalhado:

Dividido entre 31 Ações de Impacto Imediato e 54 Ações Estruturantes e agrupadas em 5 Eixos Estratégicos[10], diversas dessas iniciativas evidenciam pontos de interseção entre o estímulo ao desenvolvimento de IA e a proteção de dados pessoais.

[9] A Proposta do Plano Brasileiro de Inteligência Artificial (PBIA) foi aprovada em reunião Plenária no Conselho Nacional de Ciência e Tecnologia – CCT em 29 de julho de 2024, e será encaminhado para o Presidente da República, conforme resolução nº 4, de 08 de novembro de 2024, do Ministério da Ciência, Tecnologia e Inovação – MCTI. Publicada em: 12/11/2024. Disponível em: https://www.in.gov.br/web/dou/-/resolucao-n-4-de-8-de-novembro-de-2024-595418946.
[10] Eixo 1: Infraestrutura e Desenvolvimento de IA; Eixo 2: Difusão, Formação e Capacitação; Eixo 3: IA para Melhoria dos Serviços Públicos; Eixo 4: IA para Renovação Empresarial; Eixo 5: Apoio ao Processo Regulatório de IA.

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

De forma mais concreta, podemos citar, dentre as Ações de Impacto Imediato, as que envolvem o tratamento de dados pessoais nas áreas da Educação; Desenvolvimento Social; Indústria, Comércio e Serviços; Saúde; e Gestão de Serviços Públicos, a saber:

- Educação:
  - **Sistema Gestão Presente:** solução de IA de gestão inteligente para controle de frequência de alunos do ensino básico, visando o enfrentamento do abandono e da evasão escolar;
  - **Sistema de Predição e Proteção de Trajetória dos Estudantes:** sistema de IA para reduzir o número de alunos que abandonam escolas e universidades brasileiras por meio da identificação dos fatores de risco e/ou proteção de trajetórias por etapa;
  - **Soluções Adaptativas com IA Generativa de Avaliação Formativa e Diagnóstica para Alfabetização e Letramento**: Apoio aos professores e gestores escolares na avaliação das atividades estudantis para melhor intervenção na alfabetização.

- Desenvolvimento Social:
  - **Acredite no Primeiro Passo - IA:** plataforma que mapeia as necessidades da população registrada no CadÚnico para oferecer cursos de qualificação, oportunidades de emprego e apoio ao empreendedorismo. Implica no processamento de dados pessoais da base do CadÚnico.

- Indústria, Comércio e Serviços
  - **Inteligência Artificial para comunicação corporativa**: desenvolvimento de *chatbots* personalizados a partir de tecnologia avançada de IA para promover maior e melhor interação entre o cliente e a empresa, permitindo o aumento na quantidade de atendimentos e a redução no tempo de espera.

- Saúde
  - **Atenção Primária à Saúde Digital:** assistente de IA para otimizar a personalização do cuidado de saúde;
  - Sistema para aprimorar a precisão e agilidade nos diagnósticos médicos, particularmente em condições críticas como AVCs, pneumonia, câncer de mama, tuberculose, melanoma, entre outras;
  - Plataforma com IA para tratamento do câncer no peritônio com uso de tecnologia de ultrassom para aerossolização de quimioterápico na cavidade peritoneal;
  - Desenvolvimento de tecnologias para aprimorar a qualidade dos serviços de saúde bucal e o prognóstico de câncer oral;

- Sistema para identificar padrões anormais em faturamentos e procedimentos, ajudando a detectar e prevenir possíveis irregularidades e erros.

➢ Gestão de Serviços Públicos:

- **Fiscaliza IA - RFB (Receita Federal do Brasil):** utiliza modelos de linguagem para auxiliar na classificação e julgamento de processos administrativos tributários, incluindo pesquisa jurídica. Embora não mencione explicitamente dados pessoais, provavelmente processa informações de contribuintes nos processos administrativos fiscais;
- **Atende IA**: implementação de um *chatbot* baseado em IA na página *web* dos consulados para atendimento rápido, confiável e em qualquer idioma.

Já entre as Ações Estruturantes podem ser citados os seguintes exemplos de iniciativas de utilização de sistemas de IA e provável tratamento de dados pessoais:

➢ Eixo 3: IA para Melhoria dos Serviços Públicos

Iniciativa nº 28: Catalogação, Governança e Estratégia de Uso de Dados:
Foca em políticas de governança de dados, maturidade no uso de dados e catalogação de conjuntos de dados no governo federal;

Iniciativa nº 29: Integração e Reuso Estratégico de Dados:
Visa implementar a interoperabilidade entre órgãos governamentais para promover o compartilhamento eficiente e o reuso de dados;

Iniciativa nº 30: Personalização dos Serviços Públicos:
Busca personalizar serviços públicos para oferecer conteúdos personalizados e proativos aos cidadãos;

Iniciativa nº 31: Privacidade e Segurança da Informação no Setor Público:
Conjunto de ações que asseguram a privacidade e a segurança da informação dentro das agências federais. Implementar medidas robustas de privacidade e segurança implica manusear e proteger dados pessoais armazenados nos sistemas governamentais;

Iniciativa nº 32: Infraestrutura para Uso e Aplicação de IA na Educação:
Envolve a construção de um banco de dados unificado de dados educacionais. Esse banco de dados provavelmente conterá informações pessoais relacionadas a estudantes, professores e instituições educacionais;

Iniciativa nº 35: Desenvolvimento de IA para Aperfeiçoamento das Contratações Públicas:
Foca no desenvolvimento de ferramentas de IA para otimizar os processos de contratação pública. Contratações públicas frequentemente envolvem o manuseio de dados pessoais de licitantes, fornecedores e servidores públicos.

- Eixo 4: IA para Inovação Empresarial

Iniciativa nº 46: Retenção de Talentos para Inovação em IA:
Oferece complementos salariais para reter talentos em IA no Brasil. A administração desses complementos e o monitoramento de seus impactos provavelmente exigem o tratamento de dados pessoais dos beneficiários, incluindo informações de emprego e detalhes salariais.

Nesse mesmo sentido, a Estratégia Nacional de Transformação Digital (E-Digital), atualizada para o Ciclo 2022-2026[11], visa alinhar as iniciativas do Poder Executivo Federal no ambiente digital e aproveitar o potencial das tecnologias digitais para promover o desenvolvimento econômico-social sustentável e inclusivo, impulsionando a inovação, a competitividade, a produtividade, e o aumento dos níveis de emprego e renda.

[11] BRASIL. Ministério da Ciência, Tecnologia e Inovações. Portaria MCTI nº 6.543, de 16 de novembro de 2022. Aprova a Estratégia Brasileira para a Transformação Digital (E-DIGITAL) para o ciclo 2022-2026. Disponível em: https://antigo.mctic.gov.br/mctic/opencms/legislacao/portarias/Portaria_MCT_n_6543_de_16112022.html#:~:text=Aprova%20a%20Estrat%C3%A9gia%20Brasileira%20para,lhes%20s%C3%A3o%20conferidas%20pelo%20art.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

Estruturada em Eixos Habilitadores[12] e Eixos de Transformação Digital[13], reconhece a crescente importância tanto do tratamento de dados pessoais quanto da inteligência artificial (IA) na transformação digital do Brasil, através das seguintes ações estratégicas:

- Eixo Habilitador B: Pesquisa, Desenvolvimento e Inovação

  - Promover PD&I, inclusive por meio de encomendas tecnológicas governamentais, em temas estratégicos para a transformação digital, como Internet das Coisas (IoT), inteligência artificial, robótica, automação, computação em nuvem, *blockchain*, privacidade, segurança da informação, segurança cibernética, criptografia, *data science*, *wearables,* redes *mesh* e tecnologias alternativas e eficientes de conexão, bem como tecnologias que propiciem a economia circular de produtos e componentes eletrônicos usados.

- Eixo Habilitador C: Confiança no ambiente digital

  - Promover o fortalecimento da cultura de proteção de dados pessoais, por meio de ações estratégicas voltadas à prevenção e à detecção de infrações à LGPD, assim como ações dirigidas à capacitação e à orientação dos agentes de tratamento e da sociedade quanto às normas de proteção de dados pessoais;
  - Propor melhores práticas, códigos de conduta, monitoramento e regulamentação adequada para o uso de dados e algoritmos pelos agentes de tratamento, assim como desenvolver procedimentos com orientações éticas, atentando para os direitos fundamentais e para a transparência, inclusive na tomada de decisões pelos algoritmos e no uso de dados pelas tecnologias digitais;
  - Promover regulação adequada e proporcional aos riscos de segurança da informação, de segurança cibernética e de privacidade inerentes ao tratamento de dados pessoais que as tecnologias digitais disruptivas (inteligência artificial, *Big Data, data lake,* Internet das Coisas, computação quântica, realidade aumentada e realidade virtual etc.) possam ocasionar aos titulares.

[12] Eixos Habilitadores: A. Infraestrutura e acesso às TIC; B. Pesquisa, Desenvolvimento e Inovação; C. Confiança no ambiente digital; D. Educação e capacitação profissional; e E. Dimensão internacional.

[13] Eixos de Transformação Digital: A. Transformação digital da economia; e B. Cidadania e transformação digital do governo.

Portanto, a E-Digital estabelece o fundamento para um futuro em que IA e o tratamento de dados pessoais desempenhem um papel significativo na transformação da economia digital nacional. O foco da Estratégia em considerações éticas e governança de dados centradas no indivíduo sugere a necessidade crescente de tratamento responsável de dados pessoais e a utilização cada vez mais ampla de sistemas de IA como medidas que contribuirão, ao mesmo tempo, para a promoção do bem-estar social, com a devida proteção dos direitos individuais de liberdade, e para o desenvolvimento e crescimento do Brasil.

Por sua vez, para o desenvolvimento de modelos de Inteligência Artificial de Propósito Geral (GPAI), como grandes modelos de linguagem (LLMs) e generativos[14], frequentemente são utilizados vastos conjuntos de dados coletados de fontes amplamente disponíveis na internet e repositórios públicos. Esses dados incluem uma variedade de informações textuais, visuais, estruturadas ou não, que podem, direta ou indiretamente, conter dados pessoais.

Seguindo a linha do *EU AI Act*, um modelo GPAI é treinado com uma grande quantidade de dados, de significativa generalidade, utilizando a autossupervisão em escala e é capaz de executar, de forma competente, uma vasta gama de tarefas distintas, , e que pode ser integrado numa variedade de sistemas ou aplicações (Art. 3, nº 63).

Sobre o tema, conforme Radar Tecnológico produzido especificamente sobre Inteligência Artificial Generativa pela ANPD, [15] é comum encontrar na literatura a associação de modelos fundacionais apenas a tarefas generativas. Isto ocorre pois os modelos fundacionais são amplamente utilizados no processamento de linguagem natural para a tarefa de geração de texto. Dito isto, é importante entender que esses modelos também são utilizados em reconhecimento e classificação de imagens, conversão de fala em texto, análise de sentimentos, dentre outras tarefas discriminativas (ITI, 2023). Deste modo, não é correto assumir que os termos "modelo generativo" e "modelo fundacional" são intercambiáveis.

[14] Pesquisa realizada pela McKinsey, de 2024, aponta que 65% das organizações entrevistadas relataram seu uso regular. MCKINSEY & COMPANY. *The state of AI in early 2024: Gen AI adoption spikes and starts to generate value*. Maio de 2024. Disponível em: https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai.

[15] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Radar Tecnológico nº 3. Inteligência Artificial Generativa. Brasília, 2024. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/radar_tecnologico_ia_generativa_anpd.pdf

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

Sobre IA generativa, o mesmo estudo da ANPD delimitou quatro conjuntos de elementos que fazem parte do tratamento de dados pessoais em sistemas de IA generativa:

- Coleta e armazenamento de dados para treinamento: podem ser feitos através da raspagem de dados da *web*, que é a coleta, extração e/ou cópia automatizada de dados disponibilizados pelos usuários ou terceiros. Os dados coletados podem incluir informações como nomes, endereços, e-mails, vídeos, áudios, imagens, comentários, opiniões, preferências, entre outros. A coleta massiva de dados, como a raspagem e agregação, aumenta o risco de incluir dados pessoais.

- Processamento: acontece durante a formação da base de dados de treinamento e teste e percorre o ciclo de vida dos sistemas de IA generativa. Dados de raspagem da *web* podem ser usados e reutilizados para treinar e refinar diferentes modelos, o que pode levar a um tratamento contínuo e irrestrito de dados pessoais em diferentes sistemas. Sistemas de IA generativa geram conteúdo sintético com base nos dados de treinamento. Os modelos aprendem padrões para gerar novas representações com base nos dados de treinamento. Os dados podem não ser diretamente identificados no modelo, mas estudos recentes colocam em discussão a possibilidade de identificação de pessoas naturais por ataques de inversão de modelo. A interação com o modelo através de *prompts* pode gerar respostas com dados pessoais. O conteúdo gerado pode ser falso ou inverídico, com riscos aos indivíduos.

- Compartilhamento:
    - Compartilhamento de dados pelo usuário do sistema de IA generativa através de *prompts* que podem incluir anexos em diferentes formatos. As instruções fornecidas pelos usuários podem incluir diversos dados pessoais e sensíveis. Os usuários podem não ter conhecimento dos riscos do compartilhamento ou confiar no sistema.

    - Compartilhamento dos resultados obtidos por meio da interação com o *prompt* em sistemas de IA generativa com dados pessoais por terceiros. Os dados compartilhados podem ser reutilizados para finalidades secundárias.

    - Compartilhamento do modelo pré-treinado com dados pessoais. O compartilhamento de modelos envolve os dados que estão matematicamente presentes neles. Permite o desenvolvimento de aplicações independentes que refinam o modelo.

- Eliminação: há um desafio em delimitar o fim do período de tratamento, bem como se a finalidade ou necessidade foram alcançadas.

Importante ponderar que a discussão sobre a caraterização do uso de dados pessoais nas mais variadas fases de desenvolvimento e aplicação de modelos de IA propósito geral e de IA generativa é nova, densa e complexa. Artigo da autoridade de proteção de dados de Hamburgo (Alemanha) [16], discutindo a aplicabilidade do Regulamento Geral de Proteção de Dados (GDPR) à LLMs, ponderou que:

- Embora LLMs sejam treinados com grande quantidade de texto, incluindo dados pessoais, esses dados não são armazenados de forma direta dentro do modelo. Em vez disso, o texto é tokenizado, transformado em valores numéricos e, posteriormente, em *embeddings*[17] que capturam as relações entre esses *tokens.* Essas representações matemáticas perdem as características concretas e referências diretas aos indivíduos;

- O processo de *machine learning* transforma os dados pessoais em representações matemáticas abstratas, resultando na perda de características e referências diretas aos indivíduos. O modelo captura padrões gerais e correlações derivadas dos dados de treinamento como um todo, e não armazena os dados originais;

- Os modelos LLM não armazenam os textos utilizados no treinamento em sua forma original, e o conjunto de dados de treinamento não pode ser totalmente reconstruído a partir do modelo.

Portanto, há dúvidas consistentes com relação a quais fases do desenvolvimento e da aplicação desses modelos de IA haverá tratamento de dados pessoais, tendo a autoridade de dados de Hamburgo afirmado, ao menos, que dados pessoais não são armazenados nesses sistemas, mas apenas tratados nas fases iniciais de seu treinamento.

[16] *HAMBURG COMMISSIONER FOR DATA PROTECTION AND FREEDOM OF INFORMATION (HmbBfDI). Discussion Paper: Large Language Models and Personal Data*. 2024. Disponível em: https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/240715_Discussion_Paper_Hamburg_DPA_KI_Models.pdf

[17] Representações matemáticas (vetores) que capturam as relações aprendidas entre os *tokens.*

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

3. CONFORMIDADE LEGAL E USO ÉTICO DOS DADOS PESSOAIS NO BRASIL E EM OUTRAS JURISDIÇÕES

3.1. RISCOS E ABORDAGENS REGULATÓRIAS EM PROTEÇÃO DE DADOS

Certamente o tratamento de dados pessoais por sistemas de IA oferece avanços importantes, conforme demonstrado, mas apresenta desafios significativos à privacidade e à tutela dos dados pessoais dos indivíduos. Dentre eles são exemplos[18]:

- Coleta de dados: a IA aumenta a coleta de dados por meio de técnicas como *scraping* (coleta não consensual de dados online) e outras formas de coleta de dados "consensuais" que muitas vezes são baseadas em "ficções" de transparência ou de consentimento. A IA também torna a coleta de dados mais invasiva, pois ela pode coletar e analisar dados de diversas fontes, muitas vezes sem que as pessoas saibam ou consintam explicitamente;

- Falta de transparência: algoritmos de IA podem ser complexos e opacos, tornando difícil para os indivíduos entenderem como as decisões são tomadas e porque certos resultados são alcançados. A falta de transparência pode dificultar que as pessoas contestem decisões tomadas por IA e responsabilizem as organizações pelo seu uso;

- Geração de dados: a IA gera novos dados sobre indivíduos através da inferência, um processo pelo qual novos dados são criados a partir de informações existentes. Isso cria o que é chamado de "efeito de agregação", em que a combinação de vários "pedaços" de dados pode revelar muito mais sobre uma pessoa. A geração de dados através de inferências pode contornar muitas proteções de privacidade, pois a lei geralmente se concentra na coleta de dados prontos, ao invés de focar na sua geração;

- Conteúdo malicioso: a IA pode gerar conteúdo malicioso, como *deepfakes* e informações falsas que podem ser usadas para difamação e manipulação. A disponibilidade generalizada de ferramentas de IA aumenta o potencial de uso indevido dos dados e pode ser difícil para as vítimas buscar reparação;

- Tomada de decisões: a IA é usada para fazer previsões sobre o comportamento futuro das pessoas, o que pode levar a julgamentos e intervenções com base em ações que as pessoas ainda não cometeram,

[18] Solove, Daniel J. *Artificial Intelligence and Privacy. Florida Law Review, forthcoming January* 2025, 24 Apr. 2024.

diminuindo o respeito pela autonomia humana. A automação na tomada de decisões de IA pode levar à despersonalização e à codificação de preconceitos nas decisões;

- Vigilância: a IA torna os dados de vigilância mais pesquisáveis, compreensíveis e acionáveis, tornando a vigilância em massa mais fácil e poderosa. A identificação através de IA, como o reconhecimento facial, também pode levar a maior controle e discriminação social;

- Responsabilidade e governança: gera dificuldade em responsabilizar os desenvolvedores de ferramentas de IA e a falta de participação de diversas partes interessadas no desenvolvimento de IA pode levar a problemas adicionais de privacidade.

Em linha semelhante, estudo da *Stanford Institute for Human-Centered Artificial Intelligence* (HAI)[19] levanta as seguintes questões:

- Perda de oportunidades, liberdade e perdas econômicas. Isso pode resultar em discriminação em áreas como habitação e emprego;
- Reforço de estereótipos negativos e preconceitos. A IA pode amplificar preconceitos existentes e desigualdades;
- Danos físicos, econômicos, de reputação, emocionais e relacionais. A IA pode causar ou agravar esses danos, por exemplo, ao criar *deepfakes* que prejudicam a reputação de alguém;
- Discriminação e danos baseados na vulnerabilidade. Isso ocorre devido a assimetrias de informação entre indivíduos e coletores de dados;
- Perda de autonomia/incapacidade de fazer escolhas informadas. A falta de controle sobre como as informações são coletadas e usadas pode gerar essa consequência;
- Novos tipos de riscos baseados em identidade, inferência e agregação de dados. A IA pode inferir a personalidade e o estado emocional de uma pessoa, expondo informações pessoais sensíveis;
- Inferência de informações pessoais e criação de conteúdo difamatório;
- Sistemas de IA podem memorizar dados de treinamento e expô-los a outros usuários;

[19] King, J., & Meinhardt, C. (2024). *Rethinking Privacy in the AI Era: Policy Provocations for a Data-Centric World. Stanford Institute for Human-Centered Artificial Intelligence.* Disponível em: https://hai.stanford.edu/sites/default/files/2024-02/White-Paper-Rethinking-Privacy-AI-Era.pdf

- Sistemas de IA podem armazenar dados pessoais confidenciais para uso futuro, incluindo o re-treinamento do modelo;
- Danos à dignidade devido a preconceito e perdas de oportunidade. A IA pode levar a uma triagem e filtragem social baseada em algoritmos;
- Falta de transparência sobre como os sistemas automatizados funcionam. Isso torna difícil para os indivíduos alterarem ou limitarem seu impacto;
- Aumento da vigilância. Os sistemas de IA podem ser usados como ferramentas de controle social;
- Amplificação de vieses sociais para grupos específicos. A IA pode classificar e aplicar resultados de decisões para grandes segmentos da população com base na filiação a grupos vulneráveis;
- Ameaças à democracia. Os danos sociais podem impactar os benefícios que a privacidade oferece aos indivíduos, o que, por sua vez, impacta o desenvolvimento da autonomia necessária para os florescimentos cultural e social;
- Discriminação no acesso a oportunidades. Isso inclui empregos, habitação, educação, crédito, bens e serviços.

A Autoridade Nacional de Proteção de Dados (ANPD) também abordou alguns desses riscos no já mencionado Radar Tecnológico especificamente sobre **Inteligência Artificial Generativa** ("Radar Tecnológico nº3. ANPD, 2024")[20], como:

- **Treinamento ilegal de dados pessoais:** dados podem ser utilizados sem base legal ou sem transparência, assim como podem ter seu uso desvirtuado (como no caso de dados publicizados pelo titular e a raspagem de dados[21]), violando princípios como legalidade, finalidade e necessidade ou minimização da coleta;
- **Imprecisão de dados:** informações imprecisas ou mal gerenciadas podem levar a decisões equivocadas ou violações de direitos;
- **Vieses e decisões automatizadas discriminatórias:** dados incompletos ou enviesados podem resultar em discriminações ou danos aos titulares;
- **Exposição indevida de dados pessoais sensíveis:** modelos podem memorizar e revelar informações pessoais inadvertidamente;

[20] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Radar Tecnológico nº 3. Inteligência Artificial Generativa. Brasília, 2024. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/radar_tecnologico_ia_generativa_anpd.pdf
[21] ANPD, 2024, pág. 20.

- **Falta de segurança e de transparência:** lacunas em filtros ou falhas em controles podem expor dados pessoais a usos indevidos;
- **Produção de conteúdos sintéticos equivocados sobre uma pessoa natural (IA Gen):** O conteúdo, embora sintético, ou seja, gerado pelo modelo, apresenta narrativas que podem resultar na produção de conteúdo falso ou inverídico sobre uma pessoa real.[22]
- **Dificuldade de eliminação de dados pessoais nas IA Gen:** há um desafio em delimitar o fim do período de tratamento, bem como se a finalidade ou necessidade foram alcançadas.[23]

Complementarmente, a *Future of Privacy Forum* (FPF), acerca de LLMs, abordou os seguintes tópicos acerca dos desafios técnicos e práticos, para os quais foram propostas estratégias para melhorar a governança, salvaguardas e o equilíbrio entre funcionalidade e proteção de dados[24]:

1. Tecnologia de Transformadores e Tokenização:

   - **Riscos de privacidade no treinamento:** cada etapa do treinamento de LLMs apresenta riscos específicos que requerem estratégias de mitigação, sendo o ajuste fino mais sensível devido a possíveis dados confidenciais;
   - **Memorização e deduplicação:** LLMs podem memorizar dados quase idênticos; deduplicação ajuda, mas é subjetiva e complexa. Técnicas como privacidade diferencial podem evitar sobreajustes.

2. Treinamento e Minimização de Dados:

   - **Dados sintéticos e inferência de membros:** dados sintéticos não são ideais para testes de inferência, pois o modelo pode tratá-los como de qualidade superior ao original;
   - **Privacidade diferencial:** protege informações sensíveis, mas possui limitações práticas;
   - **Políticas de retenção:** práticas atuais incluem uso de *feedback* de usuários (positivos/negativos) como consentimento implícito para treinamento, levantando questões de privacidade.

[22] ANPD, 2024, pág. 21.
[23] ANPD, 2024, pág. 25.
[24] *FUTURE OF PRIVACY FORUM* (FPF). *Post-Event Summary and Takeaways: FPF Roundtable on AI and Privacy.* Dezembro de 2024. Disponível em: https://fpf.org/wp-content/uploads/2024/12/Post-Event-Summary-and-Takeaways-_-FPF-Roundtable-on-AI-and-Privacy-1-2.pdf.

3. Memorização, Filtros e "Desaprendizagem":

- **Desaprendizagem:** métodos para remover dados do modelo ainda são caros e em estágio inicial de pesquisa;
- **Abordagem centrada no usuário:** ferramentas para consulta e relatórios automatizados de privacidade são necessárias para maior controle individual;
- **Trocas na proteção à privacidade:** privacidade diferencial e dados sintéticos podem impactar negativamente o desempenho do modelo em casos raros, mas valiosos;
- **Consentimento e controle do usuário:** mecanismos de controle precisam ser claros, principalmente quando *feedback* é tratado como consentimento para retenção de dados;
- **Desafios do setor:** a escassez de dados abertos de alta qualidade pode aumentar a dependência de dados de usuários para treinamento.

Por sua vez, em resposta à consulta pública[25] do *Information Commissioner's Office* (ICO) do Reino Unido sobre a aplicação do princípio da limitação de finalidade no ciclo de vida da IA generativa, o CIPL (*Centre for Information Policy Leadership*[26]) apresentou suas considerações[27], destacando a necessidade de um equilíbrio entre proteção de dados e inovação tecnológica. A respeito da necessidade do uso de dados pessoais no treinamento de modelos de IA, esclareceu que isso varia consideravelmente, eis que, embora muitos modelos de IA utilizem majoritariamente dados não pessoais – como informações agrícolas, ambientais e de transporte –, alguns dependem de dados pessoais para executar funções críticas, como a redução dos vieses dos *outputs*, a compreensão de relações humanas e linguísticas. Modelos de linguagem ampla (LLMs), por exemplo, precisam de dados sobre pessoas, lugares e organizações para identificar e usar corretamente nomes próprios em contextos históricos ou atuais.

O mesmo documento destacou que a exclusão, mascaramento ou filtragem de dados pessoais podem comprometer significativamente a capacidade do modelo de compreender linguagem, afetando sua qualidade. Identificar dados pessoais em grandes conjuntos é, contudo, um desafio técnico, envolvendo questões como

[25] *INFORMATION COMMISSIONER'S OFFICE (ICO). Generative AI: Second Call for Evidence.* 2024. Disponível em: https://ico.org.uk/about-the-ico/what-we-do/our-work-on-artificial-intelligence/generative-ai-second-call-for-evidence/.
[26] *CENTRE FOR INFORMATION POLICY LEADERSHIP* (CIPL). Disponível em: https://www.informationpolicycentre.com/.
[27] *CENTRE FOR INFORMATION POLICY LEADERSHIP* (CIPL). *Response to ICO Consultation on Purpose Limitation in the Generative AI Lifecycle*. 2024b. Disponível em:https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_-_ico_consultation_on_purpose_limitation_in_the_generative_ai_lifecycle__apr_2024_.pdf

diferenciar fatos de ficção, identificar se uma pessoa está viva ou morta, ou determinar se um termo representa ou não um nome próprio. Esses obstáculos tornam complexo, em alguns contextos, o desenvolvimento de modelos robustos sem o uso de dados pessoais. Antes do desenvolvimento, salvaguardas como filtros, dados sintéticos, privacidade diferencial e criptografia homomórfica podem minimizar riscos associados a dados pessoais. Tais medidas reduzem informações sensíveis nos *outputs*, permitem treinamento sem exposição de dados reais e garantem segurança durante o processamento. A anonimização efetiva, mesmo sem eliminar completamente o risco de reidentificação, é essencial para equilibrar privacidade e funcionalidade nos modelos de IA.

Posto isso, as leis de privacidade e proteção de dados desempenham exatamente o papel de equilíbrio entre o desenvolvimento e aplicação dos sistemas de IA e a proteção de dados pessoais, de modo que se aplicarão aos sistemas de IA que envolverem dados pessoais. São exemplos, a LGPD, o GDPR, o CCPA (*California Consumer Privacy Act)*, CPRA (*California Privacy Rights Act),* leis de privacidade de outros países, como China, Japão e Singapura.

No caso da LGPD e conforme ratificado pela ANPD[28], é relevante destacar que a análise sobre a inteligência artificial e os impactos dela advindos para o tratamento de dados pessoais vão além do art. 20 e seus parágrafos, que estabelecem regras quanto à revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, a saber: ,:

Com relação aos princípios da LGPD:

(i) finalidade, que limita o uso dos dados a propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

(ii) necessidade, que requer que apenas os dados estritamente necessários sejam utilizados para alcançar as finalidades do tratamento;

(iii) qualidade dos dados, que garante aos titulares exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

[28] ANPD, 2024. Tomada de Subsídios sobre Inteligência Artificial e Revisão de Decisões Automatizadas. Disponível em: https://www.gov.br/participamaisbrasil/tomada-de-subsidios-inteligencia-artificial-e-revisao-de-decisoes-automatizadas.

(iv) transparência, que exige a disponibilização de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento; e

(v) não discriminação, que veda a realização de tratamento de dados pessoais para fins discriminatórios ilícitos ou abusivos.

(vi) responsabilização e prestação de contas, em que deve ser demonstrado, pelo agente, a 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.

No caso de bases legais:

A LGPD define hipóteses legais, previstas nos art. 7º e 11, que autorizam o tratamento de dados pessoais. Diversas hipóteses legais podem, em diferentes contextos, amparar o tratamento de dados pessoais ao longo do ciclo de vida do sistema de IA. A título de exemplo, pode-se mencionar a execução de políticas públicas, a tutela da saúde, a prevenção à fraude e a garantia da segurança do titular e a execução de contrato.

Dentre as hipóteses legais que podem ser utilizadas no contexto da IA, demandam maior discussão o consentimento e o legítimo interesse. O consentimento pode ser de difícil aplicação prática em alguns cenários relacionados a sistemas de IA. É o caso, por exemplo, da coleta de dados pessoais acessíveis publicamente mediante técnicas de raspagem de dados visando ao treinamento de sistemas de IA. Por sua vez, o legítimo interesse pode amparar o tratamento de dados pessoais para atender a interesses legítimos do controlador ou de terceiros, inclusive da coletividade. Para tanto, a LGPD exige a adoção de uma série de salvaguardas, entre as quais: a definição de medidas de transparência apropriadas e a realização de um teste de balanceamento. Uma limitação relevante para o uso da hipótese legal do legítimo interesse no contexto do uso de dados pessoais para treinamento de sistemas de IA decorre do fato de que essa hipótese legal não pode ser utilizada para fundamentar o tratamento de dados pessoais sensíveis.

No tocante a direitos dos titulares:

O uso de dados pessoais em sistemas de IA pode ter impactos significativos sobre os direitos dos titulares. Um dos aspectos mais críticos diz respeito à tomada de decisões baseadas unicamente no tratamento automatizado

de dados pessoais e que podem produzir efeitos jurídicos ou impactar significativamente os interesses dos indivíduos.

A LGPD estabelece que o titular dos dados tem o direito de entender os critérios utilizados para essa decisão e, mais especificamente, de solicitar uma revisão quando tais decisões afetarem seus interesses. Isso busca evitar ou mitigar possíveis erros, vieses ou discriminações ilícitas ou abusivas que possam surgir de decisões automatizadas que afetem negativamente o indivíduo. A utilização de dados pessoais em sistemas de IA também exige que se considere cuidadosamente os possíveis impactos negativos para o titular, os quais podem ocorrer em decisões destinadas a definir o seus perfis pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. Ainda em relação ao exercício dos direitos, destacam-se: a confirmação da existência de tratamento, o acesso aos dados pessoais, a correção de dados incompletos, inexatos ou desatualizados, a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na lei, além da possibilidade de revogar o consentimento. O titular também pode opor-se ao tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto na LGPD.
Portanto, a conformidade com a LGPD não apenas estabelece um quadro de proteção para os titulares de dados, mas também fortalece a sua confiança no desenvolvimento e no uso de sistemas de IA, assegurando que o avanço tecnológico esteja sempre alinhado à proteção dos direitos fundamentais de liberdade, incluindo, sua privacidade.

Na Europa, relatório produzido pelo *European Data Protection Board* (EDPB) sobre o ChatGPT[29] destacou que impossibilidades técnicas não justificam a não conformidade com o GDPR e apresentou uma avaliação preliminar em cinco pontos: licitude do tratamento, equidade, transparência, acuracidade dos dados e direitos dos titulares.

Sobre a licitude do tratamento, o EDPB analisou cinco etapas – coleta e pré-processamento de dados, treinamento do modelo, *prompts* e *outputs* – e ressaltou os riscos aos direitos fundamentais devido ao uso de dados coletados *online*, incluindo dados pessoais sensíveis. A OpenAI justificou o tratamento com base no legítimo interesse, e o EDPB recomendou salvaguardas, como evitar a coleta de fontes sensíveis e a realização

[29] *EUROPEAN DATA PROTECTION BOARD (EDPB). Report on the Work Undertaken by the ChatGPT Taskforce*. 23 maio 2024. Disponível em: https://www.edpb.europa.eu/our-work-tools/our-documents/other/report-work-undertaken-chatgpt-taskforce_en.

de anonimização prévia. Dados sensíveis, contudo, poderiam ser tratados como "manifestamente públicos"[30] (art. 9 (2) (e), do GDPR) e desde que garantida a conformidade por meio de filtragem adequada. Com relação à **equidade**, o EDPB afirmou que cabe à OpenAI assegurar sua conformidade com o GDPR, sem transferir essa obrigação aos usuários. Em **transparência**, destacou a necessidade de informar os titulares sobre o uso de suas interações para treinamento do ChatGPT, com exceção à raspagem impraticável de dados (art. 14 (5) (b), do GDPR). Já em relação aos **direitos dos titulares**, o EDPB reconheceu mecanismos da OpenAI, mas apontou a necessidade de aprimoramento, especialmente no direito de eliminação. Quanto à **acuracidade**, o EDPB distinguiu *inputs* (usados para treinamento probabilístico, sem necessidade de seleção factual) e *outputs*, nos quais os usuários esperam precisão. Assim, caberia à OpenAI informar sobre a natureza probabilística do sistema e sobre a possível falta de confiabilidade dos resultados, respeitando o princípio da acurácia.

Já em outra manifestação, de 18/12/2024, o EDPB estabeleceu um marco ainda mais importante ao publicar **a Opinião nº 28/2024** sobre o tratamento de dados pessoais no contexto de modelos de IA[31]. Nele apresentou os seguintes destaques:

- **Anonimização**: o EDPB considera que modelos de IA treinados com dados pessoais não podem ser automaticamente considerados anônimos. O órgão estabelece um alto padrão para anonimização, exigindo que tanto a probabilidade de extração direta (ou probabilística) de dados pessoais durante o desenvolvimento quanto a obtenção intencional ou acidental desses dados a partir de consultas sejam insignificantes. As Autoridades de Proteção de Dados (DPAs) devem analisar a documentação fornecida pelo controlador para demonstrar a anonimização, incluindo métodos usados para prevenir a coleta de dados pessoais, reduzir a identificabilidade e prevenir a extração. É necessário avaliar se dados pessoais podem ser inferidos do modelo mesmo que ele não tenha sido projetado para isso.
- **Base legal de legítimo interesse**: o EDPB reforça interpretações anteriores, mas destaca os impactos específicos das fases de desenvolvimento e implantação dos modelos de IA. Esses impactos podem variar, sendo positivos ou negativos, dependendo da natureza dos dados processados, do contexto do processamento e de suas consequências.

[30] Importante fazer a ressalva de que a LGPD não permite o tratamento de dados pessoais sensíveis com base no legítimo interesse, razão pela qual, no Brasil, outra base legal precisaria ser utilizada nesse contexto.
[31] *EUROPEAN DATA PROTECTION BOARD (EDPB). Opinion 28/2024 on Certain Data Protection Aspects.* Disponível em: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en.

- Impacto de uma potencial violação do GDPR: o EDPB define três cenários principais: (1) dados pessoais são retidos no modelo de IA e processados posteriormente pelo mesmo controlador; (2) dados pessoais são retidos e processados por outro controlador no contexto de implantação do modelo; (3) dados pessoais são processados de forma ilícita durante o desenvolvimento do modelo, mas o controlador garante que os dados sejam anonimizados antes de iniciar um novo processamento por ele mesmo ou por outro controlador. No terceiro cenário, o EDPB esclarece que, se for comprovado que a operação subsequente do modelo de IA não envolve o processamento de dados pessoais, o GDPR não se aplicaria. Assim, a ilegalidade do processamento inicial não afetaria o funcionamento subsequente do modelo. No entanto, o EDPB alerta que a separação das atividades de processamento por diferentes controladores sob o pretexto de anonimização é complexa e muitas vezes incompatível com os altos padrões estabelecidos para anonimização.
- Medidas mitigadoras: (1) pseudonimização para impedir a combinação de dados com base em identificadores individuais; (2) mascarar dados pessoais ou substituí-los por dados sintéticos no conjunto de treino; (3) estabelecer período de tempo razoável entre a coleta dos dados de treino e a sua utilização, para permitir que os titulares exerçam os seus direitos; (4) opção de exclusão, reforçando o controle dos indivíduos sobre os seus dados; (5) direito à deleção, mesmo quando os fundamentos específicos listados no Artigo 17 (1) do GDPR não se aplicarem; (6) listas de *opt-out*, que permitem que os titulares dos dados se oponham à coleta dos seus dados em certos sites; (7) impedir o armazenamento, "regurgitação" ou geração de dados pessoais (IA Generativa); (8) utilizar filtros de saída e/ou a criação de marcas d'água; (9) foco no princípio da responsabilização, que obriga os controladores a demonstrarem a conformidade com o GDPR.

Ainda no tocante à análise de riscos a titulares de dados e tentativa de mitigação no uso de sistemas de IA e tratamento de dados pessoais, estudo da CIPL, de dezembro de 2024, intitulado "*Applying Data Protection Principles to Generative AI: Practical Approaches for Organizations and Regulators*" [32], os princípios da boa-fé, finalidade, necessidade, transparência, não discriminação ilícita e da responsabilização ganham especial relevo nesse contexto, pelas seguintes razões:

[32] *CENTRE FOR INFORMATION POLICY LEADERSHIP (CIPL). Applying Data Protection Principles to Generative AI.* 2024a. Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_applying_data_protection_principles_genai_dec24.pdf.

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

- Princípios da boa-fé e da não discriminação na proteção de dados determina que as organizações tratem dados pessoais de forma equitativa, evitando resultados injustos ou discriminatórios. No contexto da IA generativa, esse princípio é essencial para garantir que os modelos não gerem resultados tendenciosos ou injustos;
- Princípio da finalidade exige que as organizações definam claramente os propósitos do tratamento de dados e evitem usos incompatíveis com a finalidade declarada. No entanto, isso pode gerar conflitos em modelos de IA generativa de uso geral, pois os desenvolvedores podem não conseguir prever ou detalhar todos os usos potenciais do modelo no momento do desenvolvimento. Assim, para o treinamento de modelos de IA generativa, legisladores e reguladores devem considerar a ampla finalidade inerente a esses modelos, projetados para responder a diferentes comandos e gerar diversas saídas. Modelos de código aberto apresentam ainda mais incertezas, já que o uso final depende dos implementadores, muitas vezes sem vínculo contratual com os desenvolvedores.
- Princípio da necessidade estabelece que a coleta de dados pessoais deve ser restrita ao necessário para uma finalidade específica, alinhando-se a conceitos como minimização de dados e proporcionalidade. Nesse particular, é importante esclarecer que os modelos de IA generativa, especialmente os de uso geral, demandam grandes volumes de dados nas etapas de desenvolvimento e treinamento, e a insuficiência de dados pode comprometer sua qualidade. Logo, aqui não significa usar menos dados do que o necessário, mas limitar a quantidade de dados pessoais ao indispensável para garantir a qualidade do modelo e adotar medidas mitigadoras de risco, como, usar dados sintéticos e limitar o tratamento a estágios específicos, implementação de filtros de saída para controle adequado de dados, de modo que o tratamento seja equilibrado com outras obrigações legais, como a segurança e confiabilidade dos produtos.
- Princípio da transparência exige que as organizações informem os indivíduos sobre a coleta e o uso de seus dados pessoais, bem como atividades de tratamento, como categorias de dados tratados. No caso de IA generativa, a transparência pode ser desafiadora devido a motivos relacionados a segredos comerciais e à natureza de uso geral dos modelos, o que pode dificultar aos desenvolvedores enumerar todas as possíveis finalidades benéficas no momento do desenvolvimento.
- Princípio da responsabilização exige que as organizações implementem medidas técnicas, contratuais e organizacionais que possam comprovar o cumprimento das exigências de proteção de dados. Leis e regulamentações que incentivam a responsabilização impulsionam as organizações a investir em programas e práticas de *accountability*, mesmo em um ambiente competitivo e em constante evolução, como no caso do desenvolvimento e da implementação de IA generativa.

Complementarmente, no que diz respeito à **aplicação do princípio da limitação de finalidade no ciclo de vida da IA generativa**, o CIPL apresentou as seguintes considerações na sua resposta à consulta pública do ICO[33]:

- **Princípio da limitação de finalidade**: destacou a relevância do princípio de limitação de finalidade para evitar o uso irrestrito de dados pessoais, mas argumentou que este deve ser complementado por salvaguardas como transparência e avaliações de riscos e benefícios, permitindo compatibilidade entre finalidades futuras e o propósito original.
- **Separação de finalidades no ciclo de vida da IA**: defendeu que o desenvolvimento de modelos de IA generativa e o de aplicações possuem finalidades distintas, mas reconheceu que podem ser integrados em alguns casos. A flexibilidade no uso contínuo de dados foi considerada essencial para a robustez e precisão dos modelos.
- **Comunicação entre desenvolvedores e aplicações**: apontou transparência como central, sugerindo a utilização de documentos como "*model cards*" para explicar o uso de dados no treinamento. No entanto, o CIPL alertou para a necessidade de proteger a privacidade dos titulares, evitando a divulgação de dados específicos.
- **Conformidade com a limitação de finalidade**: defendeu o treinamento de modelos gerais como uma finalidade legítima por si só, devido às diversas aplicações potenciais. Documentos de transparência devem delinear os usos previstos e os inadequados para o modelo.
- **Separação entre coleta de dados e desenvolvimento de modelos**: considerou coleta de dados e desenvolvimento de modelos atividades distintas, mas relacionadas à mesma finalidade, quando envolvem o treinamento de um modelo específico.
- **Documentação de finalidades:** sugeriu que desenvolvedores e implementadores descrevam claramente os propósitos do uso de dados em cada estágio, conciliando os princípios de minimização de dados com a necessidade de volumes significativos para treinamento responsável.

Por sua vez, a respeito do **legítimo interesse**, no documento *"Relying on Legitimate Interests for AI System Development"*[34], a autoridade de dados francesa (CNIL) aborda sua utilização como base legal para o desenvolvimento de sistemas de IA, especialmente quando o consentimento se torna inviável, com as seguintes considerações:

[33] CIPL, 2024b.
[34] *COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL). Relying on the Legal Basis of Legitimate Interests to Develop an AI System*. 2024. Disponível em https://www.cnil.fr/en/relying-legal-basis-legitimate-interests-develop-ai-system.

- Condições para o uso do interesse legítimo: o interesse deve ser lícito, claro, preciso, real e presente. O tratamento de dados deve ser necessário para alcançar o interesse legítimo. Não pode afetar desproporcionalmente os direitos e interesses dos titulares de dados. Exemplos de interesses legítimos: pesquisa científica, acesso à informação, aprimoramento de serviços e detecção de fraudes;
- Interesse comercial e interesse público: o interesse comercial não impede o uso do interesse legítimo, desde que haja conexão com a missão da organização e benefício para a comunidade;
- Necessidade de medidas adicionais: a implementação de medidas adicionais é crucial para mitigar os riscos e garantir o equilíbrio entre direitos e interesses. Exemplos de medidas: anonimização, pseudonimização, uso de dados sintéticos, transparência aprimorada, auditoria, e medidas para prevenir o armazenamento, regurgitação ou geração de dados pessoais em IA generativa;
- Importância da transparência e das expectativas razóaveis: a transparência é essencial para que os indivíduos compreendam como seus dados estão sendo utilizados. As expectativas razoáveis dos indivíduos devem ser consideradas ao avaliar a legitimidade do tratamento. É preciso levar em conta o contexto e as particularidades de cada caso.

- Desafios da IA Generativa: os modelos de código aberto apresentam desafios adicionais, pois o uso final depende dos implementadores. É crucial implementar medidas para prevenir usos inesperados e potencialmente prejudiciais.

Ainda sobre o tema "base legal", privilegiar o consentimento em detrimento de outras bases legais válidas, na era digital, pode gerar problemas de escalabilidade, sobrecarregar os indivíduos, causando a fadiga do consentimento, e impactar negativamente terceiros, conforme importantes conclusões da *Centre for Information Policy Leadership* (CIPL)[35], uma vez que:

- Não é escalável: a ideia de que os indivíduos podem tomar decisões para cada finalidade predefinida de processamento de dados é inadequada no mundo moderno, em que os dados são frequentemente utilizados para fins que ultrapassam a finalidade inicial de coleta. A tecnologia sempre evolui e os dados podem ter múltiplas dimensões e utilidades, o que dificulta a previsão de todos os usos futuros no

[35] *CIPL. The Limitations of Consent as a Legal Basis for Data Processing in the Digital Society.* 2024. Disponível em:https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_bkl_limitations_of_consent_legal_basis_data_processing_dec24.pdf

momento do consentimento. Além disso, o consentimento pode ser revogado a qualquer momento, o que pode dificultar a execução de contratos.

- Carga desproporcional aos indivíduos: a quantidade e complexidade da informação necessária para os indivíduos darem consentimento informado são tão grandes que se torna quase impossível para eles assimilarem tudo antes de tomar uma decisão, o que resulta no fenômeno da "fadiga de consentimento".

- Impacto negativo em terceiros: decisões de consentimento individual podem ter impacto em terceiros. Por exemplo, a necessidade de obter o consentimento para medidas de segurança cibernética e prevenção à fraude pode dificultar a capacidade das organizações de se protegerem e aos seus usuários de ataques, ou seja, dificultam a própria obediência à lei, de um modo geral. Logo, alguns tratamentos de dados com impacto em mais do que uma pessoa não deveriam depender da decisão de apenas um indivíduo.

As limitações do consentimento como base legal para o tratamento de dados, têm levado à procura de outras bases legais, como o interesse legítimo e a necessidade de dados para execução contratual. Estas alternativas podem ser mais adequadas para o ambiente digital complexo de hoje.

O interesse legítimo permite que as organizações tratem dados quando têm um interesse genuíno e válido, desde que este não prejudique os direitos e liberdades dos indivíduos. Esta base legal é acompanhada por fortes obrigações de responsabilização e avaliação de risco, garantindo a proteção dos indivíduos. Ainda, é contextual e requer uma avaliação caso a caso, permitindo flexibilidade no tratamento de dados. O indivíduo também tem o direito de se opor ao tratamento de seus dados sob o interesse legítimo.

As mudanças em outras jurisdições como o Reino Unido, EUA, Singapura e Canadá demonstram uma tendência global para afastar-se da dependência do consentimento e adotar uma abordagem mais equilibrada.

Portanto, embora o consentimento seja um elemento importante da autonomia individual, a sua aplicação excessiva pode resultar em ineficiências e dificuldades no tratamento de dados pessoais, na proteção de direitos e, até, no cumprimento, ou alcance do propósito da legislação pertinente.

Sendo assim, é importante que as organizações avaliem cuidadosamente os riscos e os benefícios de cada base legal e que adotem medidas de proteção adequadas para garantir a privacidade e os direitos dos indivíduos.

3.2. CASOS RELEVANTES DE FISCALIZAÇÃO

a. Multa e medidas de *compliance* ao GDPR a plataforma são aplicadas à empresa de *data scraping*[36]: em 05 de janeiro de 2025, a KASPR, que comercializa uma extensão do Chrome e coleta dados de contato de perfis do LinkedIn e outros sites, foi multada em €200.000 pela autoridade francesa de proteção de dados (CNIL) por violar o GDPR. As infrações incluem falta de base legal para tratamento de dados; retenção inadequada de dados; falta de transparência e desrespeito ao direito de acesso dos indivíduos. Além da multa, a CNIL determinou que a empresa pare de coletar dados de usuários com visibilidade restrita; exclua esses dados ou informe os afetados; interrompa a renovação automática de armazenamento; forneça informações claras aos indivíduos e atenda solicitações de acesso detalhando a origem dos dados. O banco de dados da KASPR contém cerca de 160 milhões de contatos usados para prospecção e recrutamento.

b. Suspensão do Tratamento de Dados Pessoais para o Treinamento de IA pela Meta[37][38]: em 02.07.24, a ANPD emitiu Medida Preventiva determinando a suspensão cautelar da nova política de privacidade do Meta, proibindo o uso de dados pessoais para o treinamento de sistemas de IA e estabelecendo uma multa diária de R$ 50 mil em caso de descumprimento. A decisão foi motivada por **indícios de irregularidades**, incluindo o **uso inadequado da base legal do legítimo interesse**, especialmente no tratamento de dados sensíveis, que podem revelar informações políticas, religiosas ou sexuais dos titulares, e a **violação das legítimas expectativas dos usuários**, que não tinham ciência de que suas informações, inclusive compartilhadas anos atrás, poderiam ser usadas para fins de IA. Além disso, a ANPD apontou a **falta de transparência**, destacando a complexidade do

[36] CNIL, 2025. *Data scraping: French SA fined KASPR €200 000*. Disponível em: https://www.edpb.europa.eu/news/news/2025/data-scraping-french-sa-fined-kaspr-eu200-000_en

[37] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). ANPD determina suspensão cautelar do tratamento de dados pessoais para treinamento da IA da Meta. 2024. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-cautelar-do-tratamento-de-dados-pessoais-para-treinamento-da-ia-da-meta.

[38] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Após pedido de reconsideração, ANPD mantém medida preventiva aplicada à Meta. 2024. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/apos-pedido-de-reconsideracao-anpd-mantem-medida-preventiva-aplicada-a-meta.

processo de *opt-out,* que cria obstáculos excessivos para o exercício dos direitos dos titulares, em desacordo com os princípios da livre acessibilidade e transparência previstos na LGPD. Houve, ainda, preocupação com a **ausência de salvaguardas específicas para dados de crianças e adolescentes**, exigindo maior cautela e controles adicionais, além de críticas ao tratamento desigual entre usuários brasileiros e europeus, onde medidas mais robustas de proteção e comunicação foram adotadas. A ANPD ressaltou que o tratamento de dados públicos deve considerar a finalidade original e propósitos legítimos específicos, demandando uma avaliação mais rigorosa, como a realização de um **Teste de Balanceamento** (LIA) e a elaboração de Relatórios de Impacto. A decisão visou evitar danos graves e irreversíveis, garantindo a **proteção dos direitos fundamentais dos titulares** e reforçando a necessidade de governança sólida e práticas alinhadas com os princípios da LGPD.

c. Investigações e Medidas contra a Plataforma X: a ANPD iniciou, em julho, uma investigação para avaliar a conformidade da plataforma X com a LGPD após ela alterar sua política de privacidade, que permitia o compartilhamento automático dos dados dos usuários para treinamento da sua IA, a Grok[39]. Em outubro, a ANPD convocou a plataforma para prestar esclarecimentos sobre as alterações nos termos de uso, que permitiriam a utilização compulsória de dados dos usuários para treinar sistemas de IA, sem consentimento explícito[40]. A ANPD destacou a urgência em receber esses esclarecimentos, devido à proximidade da data de mudança dos termos de uso, prevista para 15 de novembro[41]. Em dezembro, a ANPD notificou 20 empresas, incluindo a plataforma X, por não indicarem o contato do encarregado responsável pelo tratamento de dados pessoais, conforme exigido pela LGPD. Finalmente, em 17 de dezembro de 2024, a ANPD **determinou que a X suspendesse imediatamente o tratamento de dados pessoais de usuários menores de 18 anos** para o treinamento de sua inteligência artificial, Grok. Essa decisão foi motivada por preocupações sobre a proteção da privacidade e direitos dos adolescentes na plataforma.

[39] DUAILIBI, Júlia. ANPD convoca X para explicar mudanças em termos de uso que permitem que dados dos usuários sejam usados para treinamento de inteligência artificial. G1, 22 out. 2024. Disponível em: https://g1.globo.com/politica/blog/julia-duailibi/post/2024/10/22/anpd-convoca-x-para-explicar-mudancas-em-termos-de-uso-que-permitem-que-dados-dos-usuarios-sejam-usados-para-treinamento-de-inteligencia-artificial.ghtml

[40] Revista Fórum. ANPD convoca para esclarecer uso de dados de usuários em treinamento de IA. 22 out. 2024. Disponível em: https://revistaforum.com.br/ciencia-e-tecnologia/2024/10/22/anpd-convoca-para-esclarecer-uso-de-dados-de-usuarios-em-treinamento-de-ia-167854.html

[41] Época Negócios. X, TikTok, Uber, Cacau Show e Vivo: ANPD notifica 20 empresas por não cumprirem regra de lei de proteção de dados. Dez. 2024. Disponível em: https://epocanegocios.globo.com/tecnologia/noticia/2024/12/x-tiktok-uber-cacau-show-vivo-anpd-notifica-20-empresas-por-nao-cumprirem-regra-de-lei-de-protecao-de-dados.ghtm

d. Banimento temporário dos serviços de IA Generativa da OpenAI na Itália[42]: a autoridade de proteção de dados da Itália (Garante) baniu o ChatGPT em abril devido a várias violações do GDPR, incluindo a falta de informações adequadas aos usuários sobre o tratamento de dados pessoais, a ausência de base legal para o tratamento de dados, a incerteza sobre a precisão das informações fornecidas, a falta de verificação da idade dos usuários e a exposição potencial de menores a conteúdos inadequados. A decisão foi baseada em preocupações sobre a coleta e uso inadequado de dados pessoais e um *bug* que permitiu o acesso a informações de outros usuários.

e. Multas a empresa de reconhecimento facial: A Clearview AI, empresa especializada em tecnologia de reconhecimento facial, enfrentou três multas significativas em 2022, cada uma de €20 milhões, aplicadas pelas autoridades de proteção de dados da França[43], Itália[44] e Grécia[45]. Essas sanções resultaram de violações ao Regulamento Geral de Proteção de Dados (GDPR), incluindo a coleta e uso de dados biométricos sem consentimento, refletindo práticas de tratamento incompatíveis com os direitos fundamentais. Em 2024, a autoridade de proteção de dados da Holanda impôs uma multa recorde e está avaliando a responsabilização pessoal de executivos da empresa, reforçando a crescente pressão regulatória sobre práticas abusivas no uso de tecnologias disruptivas[46].

f. Multa a banco na Hungria[47]: em fevereiro de 2022, a autoridade nacional de proteção de dados da Hungria sancionou o Bank Zrt em aproximadamente € 653.000, por gravar e analisar automaticamente por IA as chamadas de atendimento ao cliente, classificando-os com base em sua probabilidade de insatisfação, sem

[42] G1. Itália bane ChatGPT por possíveis ameaças à privacidade. 31 mar. 2023. Disponível em: https://g1.globo.com/mundo/noticia/2023/03/31/italia-bane-chatgpt-por-possiveis-ameacas-a-privacidade.ghtml
[43] *EUROPEAN DATA PROTECTION BOARD (EDPB). The French SA fines Clearview AI EUR 20 million*. Disponível em: https://www.edpb.europa.eu/news/national-news/2022/french-sa-fines-clearview-ai-eur-20-million_en.

[44] *EUROPEAN DATA PROTECTION BOARD (EDPB). Facial recognition: Italian SA fines Clearview AI EUR 20 million*. Disponível em: https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en..
[45] E*UROPEAN DATA PROTECTION BOARD (EDPB). Hellenic DPA fines Clearview AI 20 million euros*. Disponível em: https://www.edpb.europa.eu/news/national-news/2022/hellenic-dpa-fines-clearview-ai-20-million-euros_en.
[46] *EUROPEAN DATA PROTECTION BOARD (EDPB). Dutch Supervisory Authority imposes a fine on Clearview because of illegal data collection for facial recognition*. Disponível em: https://www.edpb.europa.eu/news/national-news/2024/dutch-supervisory-authority-imposes-fine-clearview-because-illegal-data_en.
[47] *DataGuidance. Hungary NAIH fines Budapest Bank record HUF 250M fine*. Disponível em: https://www.dataguidance.com/news/hungary-naih-fines-budapest-bank-record-huf-250m-fine

informá-los claramente acerca do tratamento dos dados e sem conceder o direito de objeção ao tratamento. A autoridade destacou a importância de entender e monitorar o uso IA na gestão de dados pessoais, além de prover a necessária transparência.

g. Multa a empresas de *delivery* na Itália[48]: em julho de 2021, a Garante multou empresa de *delivery* em € 2.600.000 por violações de privacidade relacionadas ao uso de algoritmos para gerenciar seus entregadores. A empresa não forneceu transparência sobre o sistema de classificação e não implementou medidas adequadas para garantir justiça e precisão nas decisões automatizadas. A autoridade também destacou o risco discriminatório e a necessidade de proteger os direitos dos entregadores, incluindo o direito à intervenção humana.

h. Decisão da FTC sobre Cambridge Analytica[49]: nos EUA, em seu pedido final de 2019, a *Federal Trade Commission* (FTC) obrigou a empresa Cambridge Analytica a excluir ou destruir seu banco de dados pessoais, bem como o produto do trabalho, incluindo quaisquer algoritmos ou equações, originados, no todo ou em parte, a partir das informações coletadas ilicitamente em aplicativo do Facebook.

3.3. ABORDAGENS REGULATÓRIAS DOS SISTEMAS DE IA

Além das legislações de proteção de dados pessoais, há outras aplicáveis à IA euma intensa discussão global sobre novas abordagens para regular o tema, como:

- EUA- Ordem Executiva: assinada em 01 de novembro de 2023, esta espécie de decreto presidencial marca uma evolução na regulamentação de IA no âmbito federal dos EUA, ao estabelecer padrões de segurança e ações para mitigar riscos no desenvolvimento e no uso de sistemas de IA. Até então, o cenário regulatório americano era extremamente fragmentado, em razão das dificuldades de comunicação e alinhamento entre os diferentes legisladores e agências de cada ente federativo. Este documento pode representar uma migração de uma abordagem mais principiológica e baseada na autorregulação para um modelo de elenco de medidas e padrões de segurança mais específicos e mandatórios.

[48] IAPP. *Italian DPA fines food delivery app €3M for GDPR violations*. Disponível em: https://iapp.org/news/b/italian-dpa-fines-food-delivery-app-3m-euros-for-gdpr-violations
[49] *FEDERAL TRADE COMMISSION (FTC). Cambridge Analytica, LLC, Matter*. Disponível em: https://www.ftc.gov/legal-library/browse/cases-proceedings/182-3107-cambridge-analytica-llc-matter

- União Europeia (UE) – AI Act: em vigor desde 02 de outubro de 2024, esse Regulamento pioneiro, que tem servido como modelo para várias nações, estabelece uma abordagem baseada em riscos, porquanto as obrigações relativas a um sistema de IA variam de acordo com o grau de risco a ele atribuído.. Representa uma abordagem regulatória abrangente para a governança de sistemas de inteligência artificial (IA) na Europa e tem como uma de suas premissas garantir que a IA seja utilizada de forma segura, justa e respeitosa em relação aos direitos fundamentais dos indivíduos, incluindo os direitos à privacidade e à proteção de dados pessoais, uma vez que promove a conformidade com as legislações de proteção de dados, como o GDPR. Embora consideravelmente burocrático e excessivamente prescritivo, ele busca estabelecer um equilíbrio entre inovação e proteção de dados pessoais, assegurando que o uso da IA não viole direitos fundamentais na Europa.

No Brasil, além das já mencionadas políticas públicas nacionais que buscam conciliar o estímulo à utilização de sistemas de IA com o tratamento seguro de dados pessoais visando o desenvolvimento econômico nacional, em abril de 2024, o TCU analisou[50] o impacto das propostas, até então existentes, de regulação de IA[51] sobre a Estratégia Brasileira de IA (EBIA)[52], tendo destacado riscos como estagnação tecnológica, barreiras a *startups*, perda de competitividade e dificuldade de retenção de talentos. O órgão recomendou abordagem regulatória ágil, setorial e adaptável à evolução tecnológica, evitando entraves à inovação.

A interação entre regulações e políticas públicas emergentes e aquelas já existentes, tanto globais quanto nacionais, portanto, impõem desafios às empresas, que precisam desenvolver estruturas robustas para gerenciar riscos, responsabilidades e conformidade, sendo fundamental um esforço conciliatório e de harmonização que poderá ser alcançado na PNPD.

4. BOAS PRÁTICAS DE GOVERNANÇA PARA MITIGAÇÃO DE RISCOS E CONFORMIDADE LEGAL

[50] Acórdão 616/2024, Processo 033.638/2023-3. Disponível em: https://pesquisa.apps.tcu.gov.br/doc/acordao-completo/616/2024/Plen%C3%A1rio
[51] Foram avaliados os PLs 21/2020, 2338/23, 4.025/23 e 3.592/23.
[52] Instituída pela Portaria MCTI nº 4.617, de 6 de abril de 2021 e alterada pela Portaria MCTI nº 4.979, de 13 de julho de 2021. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-documento_referencia_4-979_2021.pdf

Em que pese a possibilidade de gerar riscos, como os acima apresentados, existem, em contrapartida, práticas de conformidade que se destacam no esforço de se proteger os direitos dos indivíduos, em especial sua privacidade e de seus dados pessoais, as quais devem ser incentivadas. Como exemplos, podem ser apresentadas as listadas a seguir:[53]:

a. A implementação da proteção de dados *by design* através dos seguintes meios: (i) Identificação e mitigação de riscos no tratamento de dados como vieses, discriminação e falta de transparência; (ii) anonimização: aplicação de técnicas para proteger a identidade dos titulares de dados; (iii) educação e treinamento: capacitação de funcionários para lidar com dados de maneira segura e eficiente; (iv) canais de atendimento: criação de estruturas que facilitem o exercício dos direitos dos titulares de dados;
b. A explicabilidade dos sistemas de inteligência artificial: já que a opacidade de sistemas de IA é vista como um risco significativo, técnicas de IA explicável são apresentadas como solução para tornar os processos mais transparentes, ajudando os titulares a compreenderem decisões e a exercerem seus direitos, como o direito a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais;[54]
c. Medidas para decisões parcialmente automatizadas: para decisões que combinam interação humana e automação, a LGPD exige a implementação de salvaguardas, mesmo que o direito a revisão não seja aplicável diretamente. Agentes de tratamento são responsáveis por identificar e mitigar riscos associados a essa interação;
d. Prevenção de danos sistêmicos: o artigo 49 da LGPD exige que os agentes considerem os danos sistêmicos provenientes do uso de sistemas de IA avaliando não apenas decisões individuais, mas o impacto geral da operação do sistema. Isso inclui a análise de impactos cumulativos que possam influenciar negativamente grupos ou indivíduos;
e. Auditorias e monitoramento: auditorias e relatórios de impacto são ferramentas essenciais para verificar a conformidade com a LGPD e identificar possíveis discriminações ou riscos, promovendo ajustes contínuos nos sistemas.

[53] ALMADA, Marco; MARANHÃO, Juliano. Contribuições e limites da lei geral de proteção de dados para a regulação da inteligência artificial no Brasil. Revista direito público, v. 20, p. 385-413, 2023.
[54] Artigo 20, caput, da LGPD.

No que se refere às IAs Generativas, além das medidas acima citadas, a ANPD, em seu estudo[55], acrescenta iniciativas que reforçariam a observância da legislação de proteção de dados, a saber:

- Existência de documentação adequada: a produção de documentação adequada poderia auxiliar no monitoramento dos sistemas de IA Generativa em seu ciclo de vida, de modo a identificar melhorias e permitir o exercício de direitos, no caso de existência de dados pessoais;
- Observância mais rigorosa do princípio da necessidade: o princípio não indica uma proibição em relação ao treinamento de sistemas de IA Generativa com grandes volumes de dados, mas envolve reflexões e cuidados antes do treinamento, para evitar a existência de dados pessoais não úteis nas bases de treinamento, bem como inseridos posteriormente por meio do *prompt* ou de anexos.

No caso particular de IAs generativas, o CIPL[56] também traz instruções sobre medidas de governança que podem ser adotadas para fins de compatibilização de IA generativa com a legislação de proteção de dados pessoais. Nesse sentido propugnam por uma abordagem equilibrada, contextual, baseada em risco e que, ao mesmo tempo, promova a inovação e respeite os direitos dos titulares de dados, merecendo destaque os pontos indicados a seguir:

- Extração de dados da *web*: essa prática deve conduzida de forma responsável, com salvaguardas para garantir a minimização de dados e a prestação de contas. Sugere-se que sites implementem medidas para evitar extrações excessivas ou indesejadas;
- Legítimo interesse: propõe-se a utilização da base legal do "legítimo interesse" para o tratamento de dados pessoais, especialmente no contexto do desenvolvimento de IA generativa, desde que os direitos dos indivíduos não sejam prejudicados, sopesamento que será verificado no teste de balanceamento (ou LIA – *Legitimate Interest Assessment*) e, eventualmente, na elaboração de um RIPD (Relatório de Impacto à Proteção de Dados);
- Dados sensíveis: o tratamento de dados sensíveis é reconhecido como necessário para mitigar vieses, melhorar a imparcialidade e reforçar a segurança em modelos de IA generativa, devendo ser realizado com responsabilidade e controles rigorosos para evitar acessos não autorizados. Tecnologias de aprimoramento e preservação da privacidade (PETs/PPTs), como anonimização, dados sintéticos e

[55] ANPD, 2024.
[56] CIPL, 2024a.

privacidade diferencial, auxiliam no treinamento desses modelos, promovendo diversidade de dados e reduzindo riscos associados ao uso de informações sensíveis;

- **Transparência:** documentação e proporcionalidade: medidas adequadas de transparência devem ser fornecidas pelos agentes de IA, incluindo documentação das capacidades do modelo, casos de uso pretendidos e limitações potenciais. Ademais, devem ser proporcionais ao risco do tratamento, equilibrando a compreensão do usuário com a proteção da propriedade intelectual e segredos comerciais;
- **Programas robustos de IA:** Recomenda-se que as organizações desenvolvam programas abrangentes de IA com avaliações de risco, medidas de mitigação e monitoramento contínuo.
- **Cultura de responsabilidade:** Incentiva-se a promoção de uma cultura de desenvolvimento responsável de IA nas organizações para garantir proteção de dados, precisão, justiça e transparência.

Outros instrumentos internacionais podem ser citados como exemplos de inspiração para a adoção de boas práticas e medidas éticas e responsáveis para o tratamento lícito e seguro dos dados pessoais, bem como para a governança adequada dos dados pessoais nesses sistemas. São eles:

- Diretrizes Éticas para IA confiável do Grupo de Peritos de Alto Nível em Inteligência Artificial, criado pela Comissão Europeia (8 April 2019)[57];
- Recomendação da OCDE sobre Inteligência Artificial[58];
- Princípios da IA do G20, no *Summit* de Osaka (Junho, 2019), recentemente reiterado na G20 Declaração dos Líderes de Nova Deli (Setembro, 2023)[59];
- Recomendação sobre a Ética da Inteligência Artificial da Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO, Novembro, 2021)[60];

[57] COMISSÃO EUROPEIA. *Independent High-Level Expert Group on Artificial Intelligence Set Up by the European Commission. Ethics Guidelines for Trustworthy AI.* 8 Abr. 2019. Disponível em: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419

[58] OCDE. *Recommendation on Artificial Intelligence*. Primeira adoção em 22 de maio de 2019; emenda em 3 de maio de 2024. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

[59] G20. *G20 AI Principles. Osaka Summit,* junho de 2019. Disponível em: https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/pdf/documents/en/annex_08.pdf

[60] G20. *New Delhi Leaders' Declaration*. 9 set. 2023. Disponível em: https://www.mea.gov.in/bilateral-documents.htm?dtl/37084/G20_New_Delhi_Leaders_Declaration

- A Declaração de Bletchley, adotada pelos países participantes do "*Summit* sobre a Segurança da IA" (Bletchley Park, UK, Novembro, 2023)[61];
- Declaração de Seul para IA Segura, Inovadora e Inclusiva (2023)[62];
- OECD (2024), IA, Governança de Dados e Privacidade: Sinergias e áreas de cooperação internacional [63];
- Estratégia Pan-Canadense de Inteligência Artificial (2017 e 2023)[64].

Por fim, é importante ressaltar que as tecnologias de IA, baseadas em algoritmos de aprendizagem de máquina, podem também contribuir para a privacidade e proteção de dados, uma vez que a inteligência artificial também utiliza algoritmos e tecnologias avançadas para criptografar e tornar anônimos dados pessoais de forma eficaz, permitindo análise e utilização de dados valiosos, ao mesmo tempo em que protege a privacidade. [65]

5. PRÁTICAS A SEREM IMPLEMENTADAS PARA MELHORAR A PROTEÇÃO DE DADOS E SEGURANÇA JURÍDICA NO TRATAMENTO DE DADOS PESSOAIS

[61] UNESCO. *Recommendation on the Ethics of Artificial Intelligence*. 23 nov. 2021. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000377897

[62] REINO UNIDO. *The Bletchley Declaration by Countries Attending the AI Safety Summit.* 1-2 nov. 2023. Disponível em: https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023

[63] OECD. *AI, Data Governance and Privacy*. 26 jun. 2024. Disponível em: https://www.oecd.org/en/publications/ai-data-governance-and-privacy_2476b1a4-en.html

[64] CANADA. Pan-Canadian Artificial Intelligence Strategy. Disponível em: https://ised-isde.canada.ca/site/ai-strategy/en#pillar2

[65] YANG, Le et al. *AI-Driven Anonymization: Protecting Personal Data Privacy While Leveraging Machine Learning.* arXiv preprint arXiv:2402.17191, 2024. https://doi.org/10.48550/arXiv.2402.17191

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

A OCDE também traz sugestões importantes sobre a intersecção do uso dos sistemas de IA e a proteção dos dados pessoais de modo a viabilizar o desenvolvimento econômico, tecnológico e a inovação, com destaque para:[66][67]

- *Frameworks* de privacidade são fundamentais no desenvolvimento da IA. A integração de salvaguardas de privacidade no ciclo de vida da IA promove conformidade regulatória, evita danos e impulsiona inovação responsável;
- Iniciativas tecnológicas e organizacionais para proteger a privacidade na IA: Ferramentas como dados sintéticos, tecnologias de aprimoramento de privacidade (PETs) e *sandboxes* regulatórios oferecem soluções práticas para equilibrar inovação com conformidade regulatória. Reguladores também estão implementando diretrizes específicas, como o plano de ação da CNIL e as orientações do ICO, que combinam privacidade e desenvolvimento de IA;
- Construção de confiança por meio da responsabilidade e transparência: A coleta, gerenciamento e uso responsável de dados pessoais, combinados com transparência sobre sua utilização, são elementos essenciais para criar confiança em sistemas de IA. A aplicação prática de diretrizes, como os Princípios de IA Confiável da OECD, pode harmonizar os esforços regulatórios e facilitar a criação de um ecossistema de dados baseado na confiança;
- Fomento à inovação e harmonização regulatória[68]: Embora a proteção da privacidade, da segurança e de outros direitos continue sendo primordial, as políticas também devem evitar impedir desnecessariamente a inovação responsável da IA. Isso inclui a importante etapa de permitir que pequenas e médias empresas (PMEs) responsáveis introduzam novas ofertas de IA e ampliem a concorrência. A promoção da inovação teve uma classificação alta na pesquisa da OCDE, com os membros do G7. A harmonização internacional - que inclui ferramentas amplamente disponíveis e acessíveis que podem apoiar a conformidade regulatória - pode ajudar a liberar a inovação e a concorrência da IA mantendo a privacidade e outras proteções importantes.

[66] OCDE. *Six crucial policy considerations for AI, data governance, and privacy: Insights from the OECD*. 26 jun. 2024. Disponível em: https://oecd.ai/en/wonk/six-policy-considerations-ai-data-governance-and-privacy
[67] OCDE. *A new expert group at the OECD for policy synergies in AI, data, and privacy.* 21 fev. 2024. Disponível em: https://oecd.ai/en/wonk/expert-group-data-privacy
[68] OCDE. *The AI data challenge: How do we protect privacy and other fundamental rights in an AI-driven world?.* 19 out. 2023. Disponível em: https://oecd.ai/en/wonk/the-ai-data-challenge-how-do-we-protect-privacy-and-other-fundamental-rights-in-an-ai-driven-world

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

- Harmonização de definições:[69] é necessária colaboração contínua para alinhar abordagens, integrar privacidade na IA desde o início e garantir transparência e justiça. Diferenças conceituais e terminológicas entre as comunidades de privacidade e IA geram incertezas regulatórias, conforme demonstra o quadro abaixo:

Terminology	AI policy communities	Privacy communities
Fairness	Fairness often refers to outcomes from the application of AI that are based on algorithms and datasets with **consideration for bias**, for example, through mitigating algorithmic or dataset bias for specific groups.	Fairness mainly refers to **reasonable and transparent practices**, respectful of consumers' and citizens' interests. It covers the prohibition of deceptive or misleading practices at the time of data collection, the obligation to handle people's data only in ways they would reasonably expect, and to consider how the processing may negatively affect the individuals concerned.
Transparency and explainability	Transparency, explainability and interpretability often refer to the good practice of AI **actors providing accessible information to users** to foster a general understanding of AI systems, making stakeholders aware of their interactions with AI systems, enabling those affected by an AI system to understand the outcome, and to enable those adversely affected by an AI system to challenge its outcome.	Transparency is a **positive legal obligation to inform individuals, from whom personal data are collected**, no later than at the time of data collection, on the use purposes for which consent is requested and the subsequent use is then limited to the fulfilment of those purposes.
Privacy and data protection	While the AI policy communities recognise privacy as a human right, "privacy" and "data protection" are commonly used in a narrower sense to refer to **personal information included in datasets for training AI**, and to the risks related to the loss of personal data through leakage or inference by AI models/systems.	For privacy policy communities, privacy and data protection are part of the larger, **overall human rights and consumer protection legal fabric**, covering threats to fairness, lack of transparency, and threats to data security and robustness, to be addressed through data subjects' rights, accountability, and regulatory intervention.

Sobre IA Generativa, a CIPL[70] destaca que o princípio da limitação de finalidade na proteção de dados, deve ser flexível para permitir o desenvolvimento de modelos de IA e enfatiza a necessidade de transparência e mecanismos de responsabilização, no seguinte sentido:

- O desenvolvimento de modelos de IA, de aplicações, bem como a própria aplicação de modelos de IA são propósitos distintos;

[69] *Framework exemplo: OCDE. OECD Framework for the Classification of AI systems.* 22 fev. 2022. Disponível em: https://www.oecd.org/en/publications/oecd-framework-for-the-classification-of-ai-systems_cb6d9eca-en.html.
[70] *CENTRE FOR INFORMATION POLICY LEADERSHIP (CIPL). Response to ICO Consultation on Purpose Limitation in the Generative AI Lifecycle.* 2024b. Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_-_ico_consultation_on_purpose_limitation_in_the_generative_ai_lifecycle__apr_2024_.pdf

- A coleta de dados para treinamento e o desenvolvimento do modelo devem ser considerados propósitos separados, mas relacionados;
- O treinamento de um modelo de IA generativa de uso geral é um propósito legítimo em si, pois visa capacitar o modelo a responder a diferentes comandos e gerar uma variedade de resultados possíveis;
- Embora o uso de dados pessoais seja importante, as organizações devem procurar limitar o processamento desses dados quando possível.
- Recomenda-se o uso de tecnologias de aprimoramento de privacidade (PETs), como dados sintéticos, anonimização e criptografia homomórfica, para reduzir a necessidade de tratar dados pessoais durante o treinamento;
- Desenvolvedores de modelos de IA devem ser transparentes sobre os tipos de dados pessoais usados no treinamento, incluindo metadados sobre suas características principais;
- É necessário documentar as etapas do processo de desenvolvimento do modelo e a finalidade da coleta e processamento de dados pessoais em cada etapa.

Nesse particular sobre IA generativa, segundo a ANPD, a carência de modelos abertos e detalhados no campo da IA limita oportunidades para estudos mais abrangentes para a compreensão dos impactos da IA Gen e da exploração de seu potencial inovador. Logo, a possibilidade de acesso a modelos com códigos abertos, como gradativamente vem surgindo, podem ajudar a superar essa lacuna, como o projeto OLMo (*Open Language Model*), desenvolvido pelo *Allen Institute for AI* (AI2). O OLMo fornece acesso total ao MLLE, dados de treinamento, código, pesos do modelo e documentação (AI2, 2024).[71]

6. CONCLUSÃO

O tratamento de dados pessoais em sistemas de inteligência artificial (IA) é indispensável para o desenvolvimento econômico e social do Brasil, conforme evidenciado em iniciativas como o PBIA e outras políticas públicas nacionais. A qualidade, diversidade e representatividade dos dados são elementos centrais para a eficácia dos modelos de IA, que dependam de dados bem estruturados para gerar resultados precisos e confiáveis.

Aplicações em áreas como autenticação de identidade, segurança cibernética, prevenção a fraudes, medicina preditiva, *marketing* personalizado, segurança pública e até mesmo o treinamento de IA generativa

[71] ANPD, 2024, p. 30.

exemplificam o impacto positivo do uso ético e responsável de dados pessoais. Quando conduzido com governança robusta, o tratamento de dados não só possibilita avanços sociais e econômicos, como também viabiliza políticas públicas inclusivas, reduz desigualdades, estimula a inovação e otimiza processos produtivos.

Os princípios da finalidade, adequação e necessidade, previstos na LGPD, devem ser interpretados de maneira que permitam usos futuros compatíveis com o propósito original, garantindo segurança jurídica e inovação. Embora o consentimento seja uma base legal relevante, sua priorização excessiva pode comprometer a escalabilidade dos sistemas e aplicações de IA na era digital e até mesmo comprometer o objetivo primordial das legislações de proteção de dados pela fadiga do consentimento. O interesse legítimo, quando aplicado com critérios rigorosos e medidas de mitigação de riscos apropriadas, oferece uma base flexível e equilibrada para o tratamento de dados, sem prejuízo aos direitos dos titulares, que mantêm o direito de oposição.

Nesse cenário, a LGPD confere à ANPD um papel estratégico na formulação de diretrizes que promovam a convergência de políticas públicas e incentivem o uso ético de dados pessoais para o desenvolvimento da IA no Brasil. A adoção de medidas robustas de governança, como discutido neste Estudo, deve ser vista não apenas como medida de *accountability,* mas como uma oportunidade para consolidar o país como referência em inovação tecnológica responsável. O incentivo ao tratamento ético de dados pessoais é, portanto, essencial para que o Brasil concretize políticas públicas que atendam às demandas da sociedade e impulsionem sua competitividade global.

Eventual diretriz excessivamente conservadora pode limitar o uso responsável de dados pessoais, afetando diretamente o potencial de tecnologias emergentes como a inteligência artificial. Nesse sentido, é imprescindível que a LGPD seja interpretada e aplicada com equilíbrio, promovendo uma cultura de proteção de dados que conviva harmonicamente com a inovação tecnológica, permitindo ao Brasil ocupar uma posição de destaque na economia global baseada em dados e IA.

São Paulo, 10 de janeiro de 2025.

Rony Vainzof
Conselheiro Titular do CNPD

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANEXO XIX – ESTUDO DE CASO: PREVENÇÃO A FRAUDES E AUTENTICAÇÃO/IDENTIFICAÇÃO DIGITAL

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

GT5 – Dados pessoais para o desenvolvimento econômico, tecnológico e a inovação

Subsídios para Política Nacional de Proteção de Dados e de Privacidade

Prevenção a Fraudes e Autenticação/Identificação Digital

1.1 Introdução

Nas organizações, independentemente do seu segmento e no Governo, a prevenção a fraudes se tornou tema central e prioritário, inclusive em razão dos dados pessoais, financeiros e transacionais serem elementos cruciais nas operações digitais.

As fraudes representam um dos maiores desafios para a economia global, causando enormes prejuízos financeiros e impactando a confiança em serviços digitais. Os custos financeiros com as fraudes incluem prejuízos diretos, investimentos em tecnologias de segurança para combate às fraudes e os impactos indiretos com danos reputacionais e perda de clientes.

Os prejuízos para os titulares de dados são igualmente elevados, e envolvem além dos financeiros, os emocionais.

A proteção de dados pessoais desempenha um papel fundamental, especialmente no contexto da prevenção a fraudes e segurança do titular, em que o tratamento de dados pessoais é fundamental para identificar comportamentos anômalos e prevenir a ocorrência das fraudes. Nesse sentido, O expressivo crescimento no volume de dados tratados associado ao aumento das práticas de fraudes e incidentes cibernéticos, ressalta a importância e necessidade de rígidas práticas que combinem proteção de dados, soluções de inteligência artificial (IA), de segurança da informação e conformidade regulatória.

Assim, o presente estudo tem por foco apresentar subsídios no que tange a prevenção a fraudes, considerando inclusive fator de identificação e autenticação digital com ênfase em proteção de dados pessoais alinhado às disposições regulatórias, bem como às melhores práticas nacionais e internacionais para garantir a integridade, resiliência e confiança diante das atuais ameaças e atuações fraudulentas, explora as bases legais aplicáveis no

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

Brasil e no cenário internacional, apresenta cases de uso que demonstram a relevância da Lei Geral de Proteção de Dados Pessoais para legitimar tais tratamentos e propõe pontos de melhoria

Práticas Nacionais	i. Lei nº 12.846/2013 - Lei Anticorrupção ii. Lei nº 9.613/98 – Lei de Lavagem de Dinheiro iii. Lei nº 7492/86 - Define os crimes contra o sistema financeiro nacional iv. Diretrizes de Compliance e Governança Corporativa v. Sistema de Proteção ao Crédito vi. Fiscalização da RF vii. Programa de Integridade da CGU viii. Canal de Denúncia ix. Identificação e autenticação digital por biometria x. Regras para call back diante transações financeiras fora do perfil do cliente ou movimentações suspeitas xi. Sistema para confirmação de documentos e dados (PID) Auditoria Interna e Externa xii. Resolução no. 4.893, de 26/02/2021, que dispõe sobre a Política de Segurança Cibernética e os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem. xiii. Circular no. 3.978, de 23/01/2020, estabelece procedimentos e

	controles internos a serem adotados pelas instituições financeiras para prevenção de crimes de lavagem de dinheiro e financiamento ao terrorismo. xiv. Políticas de "Conheça o seu Cliente" (KYC) xv. Resolução no. 142, de 23/09/2021, dispõe sobre procedimentos e controles de prevenção de fraudes na prestação de serviços de pagamento. As instituições devem estabelecer limites para transações, manter registros detalhados de ocorrências de fraudes. xvi. Resolução Conjunta no. 6, de 23/05/2023, estabelece requisitos para compartilhamento de dados e informações sobre indícios de fraudes entre instituições financeiras. Circular SUSEP no. 638/2021: Define requisitos mínimos de segurança cibernética para assegurar a proteção de dados pessoais tratados pelas seguradoras, entidades abertas de previdência complementar, sociedades de capitalização e resseguradores. xvii. Resolução CNSP no. 450/2022: Estabelece requisitos para credenciamento e funcionamento das sociedades processadoras de ordem

	do cliente, enfatizando condutas no relacionamento com este. xviii. Circular SUSEP no. 612/2020: Estabelece diretrizes para a prevenção à lavagem de dinheiro e ao financiamento ao terrorismo no setor de seguros.
Práticas Internacionais	i. EUA- FCPA (Foreign Corrupt Practices Act) ii. UE- GDPR iii. Reino Unido- Anti-Money Laundering (AML) – Combate à Lavagem de Dinheiro e Bribery Act iv. Austrália- Lei de Combate à Fraude e à Corrupção- Australian Federal Police (AFP) v. Canadá- Lei de Prevenção de Fraudes Financeiras (CFPOA - Corruption of Foreign Public Officials Act) vi. Singapura - Lei de Prevenção de Fraudes no Comércio Eletrônico vii. Japão- Lei de Prevenção de Fraudes Financeiras (Act on Prevention of Transfer of Criminal Proceeds) viii. Programa de Compliance e Anti Sistema de Pagamentos ix. Prevenção a Fraudes no Comércio Eletrônico x. Implementação de frameworks (Ex. Committee of Sponsoring Organizations- COSO) xi. Lei 12.965/2014 (MCI)

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

Práticas Comuns (Nacionais e Internacionais	i. Inteligência Artificial e Machine Learning ii. Canal de Denúncia iii. Auditoria Interna e Externa iv. Implantação de ferramentas tecnológicas v. ISO 27001 E ISO 27701

Abaixo segue detalhamento da prática e modo de atuação de alguns países:

1. Estados Unidos- FCPA (Foreign Corrupt Practices Act)

O FCPA é uma legislação dos EUA que visa combater a corrupção internacional e a fraude, tanto em empresas americanas como em empresas estrangeiras que fazem negócios nos EUA. É exigido que as empresas implementem controles internos eficazes para prevenir subornos e fraudes, além de garantir a transparência nas práticas contábeis e financeiras.

Modo de Operação:

- Empresas são obrigadas a manter registros contábeis precisos e a implementar controles internos para evitar pagamentos de subornos.
- Investigações de corrupção e fraudes financeiras podem resultar em pesadas multas e sanções para empresas que não seguirem as diretrizes do FCPA.
- Empresas precisam realizar treinamentos de conformidade e auditorias internas regulares.

2. Reino Unido- Regulamento de Combate à Lavagem de Dinheiro (AML)

O Reino Unido possui um conjunto robusto de regras e regulamentos relacionados ao combate à lavagem de dinheiro e financiamento do terrorismo (AML), regulados pela Financial Conduct Authority (FCA) e pela

legislação como o Proceeds of Crime Act 2002 e The Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017.

Ainda o Bribery Act 2010 segue os padrões internacionais de prevenção e combate da corrupção estabelecidos por instituições internacionais, como a OCDE.

Modo de Operação

- Instituições financeiras e outras entidades sujeitas a regulamentos devem realizar diligência devida (KYC- Know Your Customer), monitorar transações e reportar atividades suspeitas.
- Empresas devem estabelecer e manter políticas de prevenção a fraudes, incluindo a realização de auditorias de conformidade.
- Sanções rigorosas são impostas a empresas que não cumprirem as normas AML, incluindo multas pesadas e até prisão para indivíduos envolvidos.

3. União Europeia- Regulamento Geral de Proteção de Dados (GDPR)

O GDPR regulamentação da União Europeia que visa proteger dados pessoais e aumentar a segurança na forma como as empresas lidam com os dados pessoais e dados pessoais sensíveis, prevenindo fraudes como roubo de identidade e uso indevido de dados.

Na União Europeia, o OLAF (Organismo Europeu e Luta Antifraude) foi criado em 1999 para reforçar o combate à fraude e à corrupção. O seu trabalho está alinhado ao Tratado da União Europeia (TFUE), que define a proteção dos interesses financeiros da EU como prioridade. Embora seja parte da Comissão Europeia, a OLAF opera de forma independente no que se refere a investigações. O seu objetivo é garantir transparência e responsabilidade na gestão de recursos financeiros da União Europeia. Resumidamente, o seu trabalho é investigar, detectar e combater fraudes relacionadas aos recursos financeiros, combatendo irregularidades e má gestão dos recursos, além de promover políticas antifraude em toda a União Europeia. A Comissão Europeia possui diversas recomendações sobre o tema estabelecendo estratégias para o uso de dados na prevenção e combate à fraude e recomenda que os estados-membros adotem e revisem estratégias nacionais antifraude, integrando ferramentas informáticas específicas na luta contra a fraude, reforçando a análise do risco.

Modo de Operação

- Empresas são obrigadas a garantir que os dados pessoais sejam processados de forma legal e transparente, com consentimento do indivíduo.
- Os responsáveis pela segurança dos dados devem implementar medidas técnicas e organizacionais para proteger as informações pessoais contra fraudes e acessos não autorizados.
- O GDPR exige que as empresas notifiquem as autoridades e os indivíduos sobre violações de dados em até 72 horas após a descoberta do incidente.
- Penalidades severas, incluindo multas de até 4% do faturamento anual global da empresa, são aplicadas em caso de não conformidade.
- O GDPR estabelece como hipótese legal o legítimo interesse para tratamentos relacionados à prevenção de fraudes, no artigo 6.1, "f".

4. Austrália- Lei de Combate à Fraude e à Corrupção

A Austrália possui a Australian Federal Police (AFP) e outras agências que atuam no combate à corrupção, suborno e fraudes tanto no setor público quanto privado. A Australian Criminal Intelligence Commission (ACIC) também desempenha papel fundamental na prevenção de crimes financeiros, incluindo fraudes.

Modo de Operação

- Empresas e agências públicas devem adotar programas de compliance para prevenir corrupção e fraudes.
- O Criminal Code Act 1995 da Austrália tipifica crimes de fraude, incluindo o uso de informações falsas ou a manipulação de processos financeiros.
- Há um foco na cooperação internacional e na troca de informações entre países para combater fraudes transnacionais, especialmente em casos de lavagem de dinheiro e fraudes corporativas.

5. Canadá- Lei de Prevenção de Fraudes Financeiras (CFPOA- Corruption of Foreign Public Officials Act)

O Canadá adota a CFPOA para combater o suborno e a fraude em transações internacionais, além de possuir regulamentações específicas para o setor financeiro com o objetivo de prevenir fraudes bancárias e transações fraudulentas.

Modo de Operação

- A CFPOA criminaliza o suborno de funcionários públicos estrangeiros, com o objetivo de evitar fraudes relacionadas ao comércio internacional.
- Instituições financeiras canadenses são obrigadas a monitorar atividades financeiras e reportar transações suspeitas à Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).
- A implementação de medidas rigorosas de KYC (Conheça Seu Cliente) e AML é obrigatória para instituições financeiras e empresas que lidam com grandes volumes de dinheiro.

6. Singapura- Lei de Prevenção de Fraudes no Comércio Eletrônico

Singapura tem um sistema robusto para lidar com fraudes no comércio eletrônico, apoiado pela Monetary Authority of Singapore (MAS) e pela Infocomm Media Development Authority (IMDA), que regulam e monitoram as práticas de segurança digital.

Modo de Operação

- Empresas devem adotar medidas de segurança cibernética para proteger dados e transações online, incluindo a implementação de autenticação multifatorial (MFA) e criptografia.
- O governo de Singapura também promove campanhas de conscientização sobre fraudes digitais e crimes cibernéticos, educando a população sobre como se proteger contra ataques.
- Transações financeiras devem ser monitoradas de perto para identificar padrões suspeitos e prevenir fraudes de cartão de crédito e identidade.

7. Japão- Lei de Prevenção de Fraudes Financeiras (Act on Prevention of Transfer of Criminal Proceeds)

O Japão possui um conjunto de medidas legais e regulatórias para prevenir a lavagem de dinheiro, fraudes financeiras e outros crimes relacionados a transferências financeiras ilícitas. A Japan Financial Services Agency (FSA) desempenha um papel importante na regulação das instituições financeiras.

Modo de Operação

- Instituições financeiras são obrigadas a implementar políticas rigorosas de KYC e a monitorar transações para detectar atividades fraudulentas e suspeitas.
- O Japão possui um sistema de relatórios obrigatórios de transações suspeitas para ajudar a combater fraudes financeiras, incluindo a lavagem de dinheiro.
- O governo também tem investido em tecnologias como inteligência artificial para detectar fraudes e outros crimes financeiros em tempo real.

1.2. LGPD

No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD) dispõe sobre o tratamento de dados pessoais, nos meios físicos e digitais, por pessoas naturais ou jurídicas, de direito público ou privado, com o objetivo de proteger a privacidade, a liberdade.

No que tange a importância do uso dos dados pessoais para fins de proteção à fraude e segurança, não podemos nos olvidar dos fundamentos da Lei Geral de Proteção de Dados, os quais estão elencados no art. 2º., e que sinalizam os valores aos quais a norma pretende proteger. Nessa linha de raciocínio, o desenvolvimento econômico e tecnológico e a inovação estão devidamente referenciados no dispositivo legal referido, em seu inciso V, e vem ao encontro das finalidades em que os mais diversos usos de dados se dá sob a hipótese legal do art. 11, G, da LGPD.

Nesse sentido, todo o tratamento de dados pessoais precisa observar os princípios de proteção de dados, com especial ênfase, ao inciso I, e que estabelece que toda e qualquer atividade de tratamento de dados pessoais requer uma finalidade legítima e específica, além de devidamente informada ao titular. A finalidade de um tratamento impacta significativamente na escolha da hipótese legal que autoriza o respectivo tratamento de dados, tornando indispensável que os controladores tenham a ciência da responsabilidade que atraem, se porventura, utilizarem finalidades diversas daquelas que, de fato, alicerçam a escolha de uma das bases legais do art.7º. ou 11º. da LGPD. Além da observância dos princípios e da fundamentação do tratamento em uma hipótese legal, o controlador deve também assegurar os direitos dos titulares de dados pessoais e cumprir com as demais obrigações impostas pela legislação.

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

Dentre as hipóteses legais estabelecidas pela lei que podem fundamentar o tratamento de dados para fins de prevenção à fraude, destaca-se o cumprimento de obrigação legal ou regulatória, o legítimo interesse do controlador para dados pessoais não sensíveis, além de uma hipótese específica, que autoriza o tratamento de dados pessoais sensíveis, que é a prevenção à fraude e segurança do titular em sistemas de autenticação de cadastro em sistemas eletrônicos.

1.3 Casos de Uso

O uso de dados pessoais para prevenção à fraude oferece benefícios significativos ao integrar inovação e economia, pois permite a detecção de padrões de comportamentos anômalos em tempo real, reduzindo riscos de fraudes financeiras e cibernéticas. Ao promover a minimização de riscos, fortalece a segurança das transações digitais, incentivando a confiança dos consumidores em ambientes online. Permite maior eficiência operacional, ao diminuir custos com investigações e processos manuais, e, derradeiramente, contribui para a proteção das empresas e consumidores, estimulando a confiança na economia.

A autenticação robusta, com biometria multifatorial e biometria comportamental, reduz o risco de acessos indevidos, garante segurança e usabilidade, consistindo em uma das principais barreiras contra fraudes. Contudo, o tratamento de dados pessoais para prevenção à fraude não se limita apenas ao processo de autenticação, mas pode acompanhar toda a jornada do titular de dados dentro de uma aplicação, podendo tratar dados comportamentais, histórico de compras, geolocalização e identificação de dispositivos do titular.

I- Setor Financeiro e Bancário

O setor financeiro e bancário depende do tratamento de dados pessoais para fins de detecção de fraudes, sendo fundamental para proteger instituições, clientes e o ecossistema financeiro contra prejuízos decorrentes de ataques cibernéticos e violações de segurança. O tratamento de dados pessoais, neste cenário e para essa finalidade, garante confiabilidade das transações, minimiza riscos e cumpre exigências regulatórias.

I.1) Exemplos de tratamentos no setor financeiro e bancário

- Análise de Transações:

Instituições financeiras utilizam sistemas de inteligência artificial para monitorar padrões de comportamento de transações financeiras. Os dados pessoais como localização, horários e valores de transações ajudam a identificar atividades atípicas, sinalizando possíveis fraudes em tempo real.

Caso prático: Uma fraude em cartão de crédito pode ser detectada por uso simultâneo em dois países diferentes ao mesmo tempo, levando ao bloqueio do cartão até a confirmação da operação pelo titular.

- Autenticação Biométrica

Utilização de biometria através de impressão digital, reconhecimento facial ou voz, para autenticar usuários em aplicativos, garantindo que apenas o titular tenha acesso à conta.

Caso prático: Reconhecimento facial ou digital para liberação de transferências acima de determinado valor.

- Triagem de crédito e contratação de produtos

As informações fornecidas em solicitações de abertura de conta ou requerimento de crédito passam por uma triagem, cujos dados são cruzados com bases públicas e/ou internas para identificar inconsistências ou fraudes documentais.

- Prevenção de lavagem de dinheiro

As instituições financeiras são obrigadas por força de normas regulatórias advindas do Banco Central do Brasil – BCB-, a monitorar transações de alto valor ou repetitivas para identificar atividades suspeitas.

Caso prático: Um indivíduo tem os seus dados cruzados com listas de vigilância de clientes politicamente expostos (PEPs) ou de indivíduos sob sanções para fins de análise sobre possível concessão de crédito solicitado.

- Detecção de fraudes em transferências bancárias

As instituições financeiras monitoram as transferências, através do uso de tecnologias avançadas e processos automatizados para fins de detecção e bloqueio de atividades suspeitas. Esse monitoramento dos dados pessoais utiliza padrões de comportamento, análise de dados transacionais e integração com bases de dados externas para garantir segurança.

Caso prático: A instituição financeira, através do seu sistema , analisa os dados do remetente e do destinatário, tais como, nome, CPF/CNPJ, número da conta e banco, dados da transação, como valor, data, hora, finalidade e canal de operação (app, internet backing, caixa eletrônico, etc), informações do dispositivo, tais como, o modelo, sistema operacional, endereço de IP e geolocalização, e, o histórico do cliente, para comparação com os padrões de transferência anteriores e frequência de movimentações.

- Bloqueio ou retenção de transações suspeitas

As transações eventualmente sinalizadas como suspeitas podem ser bloqueadas, até o término da conclusão da análise, bem como, retidas de forma manual, por uma equipe de especialistas que avalia se a transação é legítima.

- Registro e auditoria

As instituições financeiras por força regulatória armazenam os "logs" de todas as transações, incluindo as suspeitas e os motivos de bloqueio, para auditoria futura. Os dados coletados ajudam a refinar os algoritmos e atualizar as regras de monitoramento.

- Implementação de medidas de segurança para evitar vazamento de informações

O sistema financeiro requer a implementação de medidas de segurança por parte das instituições financeiras para fins de mitigação de riscos envolvendo dados pessoais dos titulares. O Banco Central do Brasil, órgão regulador, estabelece diretrizes para que as instituições financeiras assegurem a proteção dos dados pessoais de seus clientes. Essas orientações estão alinhadas à Lei Geral de Proteção de Dados Pessoais – LGPD- e visam garantir a segurança e a privacidade das informações no âmbito do Sistema Financeiro Nacional.

Caso Prático: Em janeiro de 2002, o BCB, informou um vazamento de dados de aproximadamente 160 mil chaves PIX vinculadas à empresa Acesso Soluções de Pagamento, instituição de pagamento autorizada. As informações vazadas incluíam dados cadastrais como nome, CPF e dados bancários. A causa do incidente se deu em função do sistema de acesso de permissões de usuários não autorizados.

https://g1.globo.com/economia/pix/noticia/2022/02/03/pix-quais-dados-foram-vazados-quais-os-riscos-e-como-se-proteger.ghtml?UTM_SOURCE=outlook&UTM_MEDIUM=share-bar-

app&UTM_CAMPAIGN=matérias

Principais Instruções do Bacen:

https://www-correiobraziliense-com-br.cdn.ampproject.org/c/s/www.correiobraziliense.com.br/cidades-df/2024/11/amp/6993331-pcdf-bloqueia-rs556-mil-de-quadrilha-especializada-em-golpes-ciberneticos.html

II- E-commerce

O uso de dados pessoais para prevenção à fraude no e-commerce é de grande relevância para garantia da segurança das transações, proteção dos consumidores, evitando assim, prejuízos financeiros às empresas. A manutenção da confiança dos consumidores permite o crescimento da economia, uma vez que, sentem-se seguros na utilização dos sistemas. Por sua vez, a minimização de perdas financeiras, causados por prejuízos em decorrência de "chargerbacks", devoluções fraudulentas e uso indevido de cupons produzem maior segurança jurídica aos atores que atuam neste mercado.

II.1) Exemplos:

- Prevenção à Fraudes em Pagamentos Online

A utilização de dados pessoais, como endereços de IP, histórico de compras e geolocalização são importantes para que as plataformas de e-commerce identifiquem compras fraudulentas.

Caso prático: O bloqueio de uma transação através de bloqueio de sistema quando for realizada por um dispositivo nunca utilizado e proveniente de uma região de alto risco.

Caso Prático: Em 2019, a empresa de e-commerce Netshoes enfrentou um incidente de segurança que resultou na exposição de dados de 2 milhões de clientes na internet, incluindo nome completo, CPF, e-mail e histórico de compra.

https://g1.globo.com/tecnologia/noticia/2024/07/17/netshoes-diz-que-dados-de-clientes-

podem-ter-sido-vazados-apos-incidente-cibernetico.ghtml

Caso Prático: Em outubro de 2021, uma falha de segurança na plataforma brasileira Hariexpress expôs mais de 1,7 bilhão de dados de clientes e lojistas cadastrados em sites de comércio eletrônico.

https://exame.com/tecnologia/entenda-caso-hariexpress-megavazamento/

- Análise comportamental de usuários

Com base no histórico do cliente, o sistema identifica os padrões normais de transações, frequência, valores e tipos de produtos possibilitando a identificação de anomalias que apontam para possíveis fraudes.

- Verificação de identidade

As plataformas podem exigir a depender do valor da transação, validação adicional do usuário. Exemplo clássico desta situação se dá quando é requerido ao consumidor/titular de dados pessoais, uma selfie acompanhada do documento de identidade para validação da sua identidade.

- Controle de fraudes em cupons e promoções

As plataformas para fins de coibir fraudes com a utilização de múltiplas contas para cupons ou promoções, processam dados pessoais como IP, dispositivos usados, e-mails e método de pagamento.

Caso Prático um cliente criando várias contas e usando o mesmo dispositivo para obtenção de descontos repetidamente poderá ter a sua conta bloqueada.

- Rastreamento de logística e entregas

As plataformas em seus sistemas de disputas on-line (ODRs) seguidamente são demandadas por reclamações envolvendo fraudes relacionadas a falsas reclamações de não recebimento de produtos. O uso de rastreamento em tempo real, endereço de entrega e análise do histórico de compras e reclamações anteriores para validar se um cliente recebeu ou não o produto é de suma importância para a resolução da reclamação.

- Prevenção de fraudes de reembolso e chargerback

As plataformas seguidamente estão envolvidas com reclamações de clientes mal-intencionados que solicitam reembolsos indevidos alegando que não autorizaram as compras.

Nesses casos, sistemas verificam se o dispositivo utilizado na compra é o mesmo que o cliente geralmente utiliza em suas transações, bem como, geolocalização, histórico de compras e métodos de pagamento. Portanto, evita-se através da análise dos dados pessoais do consumidor/titular destes dados, que empresas sejam prejudicadas com cancelamento e devoluções de valores, as quais não deram causa.

- Validação de dados de cadastro

As plataformas precisam validar o cadastro de dados realizados para fins de identificar incorreções que possam gerar fraudes, incluindo a lavagem de dinheiro. Nesse sentido, os sistemas identificam se o CPF informado no cadastro é válido e associado ao nome e endereço fornecido pelo indivíduo.

III- Companhias Aéreas

O tratamento de dados pessoais no setor das companhias aéreas com a finalidade de prevenção à fraude e de segurança é uma prática comum, devido a necessidade de garantir a segurança dos passageiros e o cumprimento de normas regulatórias.

III.1) Exemplos:

- Verificação de identidade no Check-In

As companhias aéreas utilizam sistemas de validação de identidade para verificar os dados dos passageiros no momento do check-in. Informações pessoais, como nome, número do passaporte ou documento de identificação, são cruzadas com bancos de dados governamentais ou listas de vigilância para prevenir atividades fraudulentas ou ameaças à segurança.

- Análise de transações

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

As companhias aéreas analisam dados de compra online, tais como, pagamentos realizados com cartões de créditos roubados, múltiplas passagens compradas com o mesmo cartão para destinos diferentes em um curto espaço de tempo.

-Análise de atividades suspeitas

As companhias aéreas analisam dados como endereço de IP, geolocalização, e histórico de compras são utilizados para identificação de atividades suspeitas.

-Verificação de dados pessoais para consulta em listas de proibição de passageiros (Uso de APIs para Screening)

Os dados dos passageiros são enviados para verificação em listas de restrição, como a
No-Fly List, nos EUA. Os dados do passageiro são comparados com listas de terroristas, criminosos procurados ou pessoas com proibições legais de viajar. Essa troca de informações ajuda a identificar pessoas que representam riscos à segurança antes do embarque.

*Screening é o processo de verificação ou triagem de informações para identificar riscos, irregularidades ou inconsistências em um determinado contexto. Os dados são coletados, cruzados, analisados manual ou automaticamente e é tomada uma decisão com base no resultado do screening.

- Reconhecimento Facial e Biométrico

Muitas Companhias Aéreas implementam tecnologias de reconhecimento facial e biometria no embarque e no controle de fronteiras. O objetivo é comparar as imagens capturadas com os dados armazenados em passaportes biométricos e bancos de dados governamentais para prevenir fraudes de identidade e consequentemente prática de crimes.

- Monitoramento de comportamentos em aeroportos

Os aeroportos, utilizam sistemas de segurança dentro destes espaços, com câmeras e inteligência artificial para monitorar o comportamento de passageiros, com o objetivo de detectar preventivamente comportamentos anormais e consequentes riscos à segurança.

- Gestão de Bagagem

Informações vinculadas ao registro de bagagens para evitar fraudes, como o uso de etiquetas falsas para retirar pertences de outro passageiro ou possibilitar a troca proposital de bagagem. Algumas companhias aéreas utilizam QR codes ou tecnologia RFID para rastrear bagagens associadas a dados específicos do cliente.

- Programas de Fidelidade

Dados pessoais de clientes inscritos em programa de fidelidade são analisados para identificar possíveis fraudes, como transferências de milhas não autorizadas ou uso indevido de benefícios.

- Prevenção de Ataques Cibernéticos

Companhias aéreas monitoram atividades nos sistemas de reservas e contas de usuários para prevenir roubo de dados pessoais ou informações financeiras. Autenticação de identidade e análise comportamental são usados para identificar tentativas de acesso não autorizadas.

Caso Prático: A LATAM Airlines, em 2021, informou que parte dos membros de seu programa de fidelidade, o LATAM Pass, teve dados pessoais expostos devido a um ataque cibernético sofrido pela empresa de tecnologia SITA, que prestava serviços ao setor aéreo.

https://valor.globo.com/empresas/noticia/2021/03/13/ataque-hacker-expe-dados-de-passageiros-da-latam-no-brasil.ghtml

IV- Mercado de Seguro

O tratamento de dados pessoais no ramo de seguros detém importância significativa, uma vez que fraudes neste ambiente, podem gerar prejuízos milionários para as empresas, bem como, aos segurados. A análise de dados pessoais permite a identificação de comportamentos suspeitos, reduzindo pagamento indevido de indenizações fraudulentas.

As seguradoras também são obrigadas por regulamentações específicas do Órgão Regulador, a SUSEP, a adotar medidas de segurança e prevenção à fraude, além, das obrigações impostas pela Lei Geral de Proteção de Dados. Menores custos operacionais, preços mais competitivos, maior precisão na análise de sinistros e

desenvolvimento de produtos personalizados, são alguns dos benefícios do tratamento de dados pessoais para fins de prevenção à fraude e segurança.

IV-1) Exemplos:

- Detecção de Fraudes em Sinistros

As seguradoras analisam os dados pessoais, histórico de sinistros e padrões de comportamento para identificar possíveis fraudes em pedidos de indenização.

- Emissão de Apólices Falsas

Criminosos utilizam dados pessoais obtidos ilegalmente para emitir apólices de seguros fraudulentos, cobrando prêmios sem cobertura válida.

- Solicitações de contratos e boletos fraudulentos

Fraudadores se passam por corretores de seguros, utilizando dados pessoais roubados
para enviar contratos e boletos falsos aos consumidores. Ao pagar por esses documentos. As vítimas acreditam estar contratando um seguro legítimo, mas acabam sendo lesadas financeiramente.

Caso Prático: Em abril de 2023, foi reportado um vazamento que expôs mais de 5,8 milhões de registros de saúde de brasileiros, incluindo consultas, procedimentos e exames realizados por uma importante seguradora nacional. As informações abrangiam dados pessoais como nomes, CPFs, data de nascimento, e detalhes de planos de saúde entre 2016 e 2020. O vazamento de dados foi atribuído a empresa Porto Saúde.

https://canaltech.com.br/seguranca/vazamento-expoe-quase-6-milhoes-de-dados-de-saude-dos-brasileiros-246314/

Caso Prático: Em novembro de 2020, a seguradora Prudential do Brasil comunicou um
incidente de segurança que permitiu que uma pessoa não autorizada copiasse informações relacionadas a propostas de contratação de serviços, resultando no vazamento de dados pessoais de clientes.

https://www.cisoadvisor.com.br/seguradora-prudential-tem-dados-roubados-em-ciberataque/

V- Tecnologia e Mídias Sociais

O tratamento de dados pessoais para fins de prevenção à fraude na tecnologia e nas mídias sociais é de suma importância para proteger usuários, plataformas e anunciantes contra atividades maliciosas e fraudulentas, como o roubo de identidade, criação de contas falsas e golpes financeiros. Esse tratamento contribui para a confiança nas plataformas e para a segurança dos seus usuários e das interações que ocorrem nestes ambientes virtuais. O objetivo é proteger o usuário, procurando impedir que sejam vítimas de golpes, como phishing, roubo de contas ou fraudes financeiras, entre outros, reduzindo perdas financeiras, por fraude publicitária, roubo de serviços ou uso indevido das funcionalidades. Promove-se, assim, o aumento da confiabilidade de um ambiente digital e seguro, essencial para a continuidade das operações e engajamento dos usuários.

V.1) Exemplos:

- Autenticação de identidade para detecção e bloqueio de contas falsas

As plataformas como Facebook, Google, Instagram, Microsoft fazem uso de dados pessoais, tais como, números de telefone, reconhecimento facial, verificação em duas etapas, para assegurar sobre a identidade do usuário e prevenir fraudes, através da sua autenticação segura.

Caso Prático: O bloqueio de contas por detecção de tentativas de acesso a partir de dispositivos e localização não reconhecidos.

Caso prático: Uma conta que interage em massa com milhares de perfis em minutos pode ser bloqueada por apresentar comportamento típico de “bots”.

- Prevenção de fraude publicitária

As plataformas monitoram curtidas e impressões de anúncios para identificar “click fraud”, cliques maliciosos feitos por “bots” ou concorrentes, processando dados pessoais como endereço de IP, dispositivos, geolocalização e padrões de curtidas.

- Combate ao “phishing” e links maliciosos

Os links compartilhados em mensagens e postagens são analisados para identificar conteúdos fraudulentos, evitando assim, que os usuários sejam vítimas de golpes financeiros.

Caso prático: Um usuário envia um link que redireciona a uma página falsa de login, terá esse link bloqueado pelo Instagram, mesmo que seja feito através de uma mensagem direta.

- Análise comportamental dos usuários

As plataformas sociais utilizam inteligência artificial para identificar comportamentos fora do padrão, como curtidas ou comentários em massa.

Caso prático: Um usuário começa a seguir milhares de perfis em minutos. A conta é temporariamente bloqueada até posterior confirmação de identidade deste.

- Monitoramento de conteúdo e comentários

Os comentários e postagens são analisados pelo sistema com inteligência artificial para identificar “spam” ou conteúdos que possam envolver fraudes, discurso de ódio e inúmeros outros ilícitos.

Caso prático: As plataformas através da análise de textos das postagens, frequência de publicação e padrões linguísticos do usuário, podem excluir links repetidos para promoções falsas.

VI- Setor Público:

O tratamento de dados pessoais para prevenção à fraude no setor público é de grande relevância para fins de garantir a integridade dos recursos públicos, evitar desvios financeiros, proteger cidadãos e promover a transparência nos serviços governamentais. A fraude no setor público é de extrema nocividade pois além de prejuízos econômicos, abala a confiança da sociedade e compromete os programas sociais.

VI.1) Exemplos:

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

- Prevenção de Fraudes em Benefícios Sociais

Os dados dos indivíduos são processados e analisados pelo Governo para análise de informações de beneficiários para identificar inconsistências ou informações duplicadas.

Caso Prático: Programas de combate à fraude no INSS, que cruzam informações para evitar pagamentos indevidos de pensões ou aposentadorias.

- Detecção de fraudes em licitações

Os sistemas monitoram concorrências públicas para identificar irregularidades, como vínculos entre empresas participantes, através da participação societária dos sócios.

- Prevenção de fraude em impostos

O setor público, através de seus órgãos fiscais, como a Receita Federal, cruza informações para identificar inconsistências em declarações de renda ou pagamentos
tributários a menor.

Caso prático: A detecção de incompatibilidade entre a renda declarada e o patrimônio do contribuinte, através do cruzamento de informações, como renda declarada, movimentação bancária e patrimônio.

- Monitoramento de fraudes em programas habitacionais

O setor público analisa dados dos candidatos a programas como o “Minha Casa Minha
Vida” para evitar fraudes, como a inclusão de pessoas com imóveis próprios, situação vedada para a concessão deste programa.

Caso prático: Os dados de um candidato a obtenção de um financiamento pela modalidade do programa “Minha Casa Minha Vida” são analisados e verificados em cartórios para confirmar a inexistência de propriedade em nome do solicitante, ratificando assim a sua elegibilidade.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

Como visto são muitos os setores e casos de uso de dados pessoais para prevenção a fraudes. Nesse sentido, é inconteste a importância do arcabouço regulatório da LGPD e das demais normas setoriais aplicáveis para a prevenção, detecção e combate às fraudes. Contudo, muitas vezes, o tratamento de dados e a eficácia das soluções técnicas e administrativas para prevenção à fraude encontra limitação na falta de conhecimento dos agentes de tratamento sobre as práticas legítimas de tratamento de dados para essa finalidade. A falta de uma cultura forte de proteção de dados em nossa sociedade também é uma limitação para os titulares de dados reconhecerem práticas lícitas e se insurgirem contra as ilícitas.

Nesse sentido, sugere-se:

- Investimento em educação e capacitação, conscientizando agentes de tratamento e titulares sobre a importância do tratamento adequado de dados pessoais, com transparência e respeito aos direitos dos titulares e demais regramentos estabelecidos pela LGPD, incentivando as práticas legitimas de tratamento de dados pessoais.

- Incentivo à inovação e pesquisa fomentando o desenvolvimento de soluções baseadas em inteligência artificial e biometria comportamental, aumentando a segurança no tratamento de dados, protegendo os titulares e contribuindo para o desenvolvimento de um ambiente digital confiável e competitivo, com total conformidade à LGPD.

Débora Sirotheau Siqueira Rodrigues

Myreilla Aloia T P da Cruz

Com contribuições da especialista Martha Leal, vice-presidente do INPD, encaminhadas via ofício pela entidade.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANEXO XX – ESTUDO DE CASO: PROTEÇÃO AO CRÉDITO

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ESTUDO DE CASO: PROTEÇÃO AO CRÉDITO

Conselheiro: Rony Vainzof[72]

1. INTRODUÇÃO

1. O tratamento e a proteção de dados pessoais desempenham um papel essencial na proteção ao crédito, servindo como base para avaliar a capacidade financeira da sociedade na economia nacional. Esse processo permite gerar eficiência contínua em relação à capacidade de pagamento e ao cumprimento de obrigações financeiras, favorecendo a sociedade e a saúde do sistema econômico brasileiro.

2. Regulamentada, de modo geral, pelo Código de Defesa do Consumidor e mais recentemente pela Lei Geral de Proteção de Dados Pessoais (LGPD), e de forma específica, pela Lei de Cadastro Positivo e por órgãos como o Banco Central do Brasil e o Conselho Monetário Nacional[73], a proteção ao crédito busca equilibrar a privacidade e a proteção de dados dos indivíduos com os interesses econômicos e sociais do Brasil e das instituições que operam nesse mercado, promovendo eficiência econômica, desenvolvimento sustentável, segurança jurídica e proteção aos direitos e garantias fundamentais dos indivíduos.

3. Ou seja, a proteção ao crédito, embasada em dados pessoais, é essencial para o funcionamento de uma economia moderna. No Brasil, onde o crédito é um motor significativo do crescimento econômico, garantir um equilíbrio entre proteção ao crédito e proteção de dados pessoais é fundamental. Isso requer não apenas uma regulação eficiente, mas também a implementação de práticas éticas e transparentes por parte das empresas que operam nesse setor.

2. A IMPORTÂNCIA DOS DADOS PESSOAIS PARA A PROTEÇÃO AO CRÉDITO

4. Os dados pessoais são fundamentais para sistemas de proteção ao crédito pois permitem:

- Avaliação de Risco de Crédito: informações como histórico financeiro, hábitos de pagamento e renda são essenciais para que instituições financeiras e empresas avaliem o risco de inadimplência.

[72] Conselheiro Titular do CNPD. O trabalho contou com o apoio dos pesquisadores Verônica Barros e Mateus Lamonica.
[73] O Conselho Monetário Nacional (CMN) é o órgão deliberativo máximo do Sistema Financeiro Nacional, conforme site do Ministério da Fazenda em: https://www.gov.br/fazenda/pt-br/assuntos/cmn/atuacao-da-spe#:~:text=O%20CMN%20estabelece%20as%20diretrizes,e%20fiscaliza%C3%A7%C3%A3o%20das%20institui%C3%A7%C3%B5es%20financeiras.

- Decisões Justas e Personalizadas: o uso de dados pessoais promove decisões baseadas em critérios objetivos, como histórico de pagamentos, reduzindo discriminações arbitrárias.

- Inclusão Digital e Econômica: acesso a bancos de dados de qualidade, precisos e atualizados evitam práticas abusivas e promovem acesso ao crédito para a população, especialmente para os grupos mais vulneráveis e desbancarizados, permitindo que indivíduos sem histórico de crédito, mas com comportamento financeiro responsável, acessem melhores condições.

5. A análise de crédito desempenha papel crucial em vários aspectos da economia e da sociedade brasileira, como:

- Consumo: o crédito é um dos motores que permite o consumo no Brasil, responsável por alavancar setores como o varejo, construção civil e serviços.

- Pequenos Negócios: o crédito é uma das principais fontes de financiamento para micro e pequenas empresas.

- Inovação: *startups* e empresas inovadoras frequentemente dependem de crédito para investir em tecnologia e expansão.

- Redução das Taxas de Juros: uma análise de crédito eficiente possibilita taxas mais justas, alinhadas ao perfil de risco do tomador, reduzindo o "spread bancário".

- Geração de Empregos: empresas financiadas criam empregos diretos e indiretos.

- Prevenção de Endividamento Excessivo: uma análise de crédito responsável evita a concessão de crédito para indivíduos ou empresas com capacidade financeira insuficiente, protegendo os consumidores de situações de endividamento excessivo.

6. Estudo recente realizado pela Febraban[74] mostra que a inadimplência é a principal vilã para o aumento dos juros básicos do Brasil, ou seja, do custo do crédito. O Banco Central do Brasil (2024)[75], por sua vez, afirma que para a redução sustentável do custo do crédito são necessárias ações para diminuir a inadimplência, melhorar a recuperação de garantias e reduzir assimetrias de informação. Dados precisos e de qualidade, inclusive pessoais, são essenciais para estimar com exatidão o custo do crédito e torná-lo menos oneroso[76].

[74] "Como Fazer os Juros serem mais baixos no Brasil". Disponível em: https://cmsarquivos.febraban.org.br/Arquivos/documentos/PDF/Juros%20Mais%20Baixos%202.pdf
[75] Disponível em: https://www.bcb.gov.br/conteudo/home-ptbr/TextosApresentacoes/Apresentacao_RCN_Cadastro_Positivo_VPUB.pdf
[76] Agenda Microeconômica BACEN, 2024.

7. Nesse contexto, diversos outros estudos e relatórios de instituições brasileiras oficiais ou empresas privadas que atuam nesse mercado confirmam a importância da Lei do Cadastro Positivo. O Relatório de Análise do Banco Central, de abril de 2021[77], a Agenda Microeconômica e de Inovação do Banco Central do Brasil[78], bem como um estudo recente da Serasa[79] são exemplos de documentos que trazem informações relevantes sobre os benefícios que foram gerados pela Lei, a saber:

8. Para os indivíduos:

- Acesso mais facilitado ao crédito: aproximadamente 41% das pessoas físicas cadastradas migraram para faixas de menor risco de crédito, resultando em maior facilidade de acesso ao crédito com condições mais favoráveis, como menores taxas de juros. (BACEN, 2024)
  Em cinco anos de vigência do modelo de adesão automática ao Cadastro Positivo, a possibilidade de uma pessoa negativada ter acesso a um crédito de qualidade passou de 0,5% para 8,5%, um crescimento de 17,5 vezes. O Cadastro Positivo também impactou pessoas que tiveram seus restritivos resolvidos, em cerca de três vezes. Em um cenário sem esse Cadastro, apenas 7,3% dos consumidores teriam chances de acesso a um crédito mais qualificado, enquanto, atualmente, o percentual atinge 20,7%. (Serasa, 2024). Segunda a ANBC[80], a implantação do Cadastro Positivo trouxe um aumento de 78% na nota de crédito dos consumidores. Além disso, aumentou a visibilidade de 21 milhões de pessoas físicas e jurídicas que, por não terem uma conta junto a instituições financeiras – os chamados desbancarizados – eram totalmente invisíveis ao mercado de crédito.

- Redução de taxas de juros: houve redução média de 10,4% nos *spreads* das operações de crédito pessoal para novos tomadores com pontuações do Cadastro Positivo. (BACEN, 2024)

- Jovens especialmente beneficiados: pessoas com menos de 30 anos foram as mais beneficiadas, com 59% delas migrando para faixas de menor risco. (BACEN, 2024)

[77] "Análise dos Efeitos do Cadastro Positivo, abril, 2021. Disponível em: https://www.bcb.gov.br/content/publicacoes/Documents/outras_pub_alfa/analise_dos_efeitos_do_cadastro_positivo.pdf
[78] "Agenda microeconômica e de inovação do Banco Central do Brasil", agosto, 2024. Disponível em: https://www.bcb.gov.br/conteudo/home-ptbr/TextosApresentacoes/Apresentacao_RCN_Cadastro_Positivo_VPUB.pdf
[79] "Cadastro Positivo amplia em 18 vezes as chances de acesso ao crédito para negativados.", de 29.08.24. Disponível em: https://www.serasaexperian.com.br/sala-de-imprensa/servicos-de-credito/cadastro-positivo-amplia-em-18-vezes-as-chances-de-acesso-ao-credito-para-negativados-segundo-estudo-realizado-pela-serasa-experian/
[80] Em resposta ao ofício deste GT5 do CNPD, solicitando contribuições.

9. Para o país:

- **Diminuição da inadimplência e prevenção do superendividamento:** benefícios que ainda podem ser potencializados com a continuidade de adesão de novas fontes de dados, como contas de saneamento básico e energia (BACEN, 2024)[81].

- **Importância do uso de informações sobre crédito pelas MPMEs:** No segmento de crédito a micro, pequenas e médias empresas (MPME), 88% das instituições mostraram interesse no uso destas informações, sendo que a maior parte delas indica que ainda está realizando ajustes para utilização dos dados, ou que pretende realizar futuramente. (BACEN, 2024)

- **Impacto na migração de faixas de risco para pessoa jurídica:** para os cadastrados pessoas jurídicas, 30% se beneficiaram com migração para faixas de menor risco, metade manteve a faixa de risco e 20% passaram a faixas de maior risco. (BACEN, 2024)

- **Crescimento do crédito às empresas e relação com o PIB:** o aumento do volume de crédito às empresas foi de 4,5% em 2023 – ante um crescimento de 10% em 2022. Medido como proporção do PIB, o saldo total de crédito, incluindo pessoas físicas e jurídicas ficou praticamente estagnado, sendo estimado em 53,2%. Isso significa que, em termos reais, o crédito cresceu no mesmo ritmo que a economia. Essa relação fornece uma medida da presença do crédito nas atividades econômicas do país. (ANBC, 2024)[82]

10. Conforme apontado pela CONEXIS[83], o Instituto Locomativa estimou que, em 2021, cerca de 34 milhões de brasileiros eram desbancarizados ou pouco utilizavam suas contas bancárias[84]. Já uma pesquisa do Instituto Dom Cabral em parceria com a BRINKS[85] apontou que 38,5% da população brasileira não tinha conta bancária

[81] "Agenda microeconômica e de inovação do Banco Central do Brasil", de 08.08.24. Disponível em: https://www.bcb.gov.br/conteudo/home-ptbr/TextosApresentacoes/Apresentacao_RCN_Cadastro_Positivo_VPUB.pdf
[82] "O tamanho do crédito: revisitando a relação crédito-PIB no Brasil", ANBC – Associação Nacional dos *Bureaus* de Crédito. Disponível em: https://anbc.org.br/o-tamanho-do-credito/
[83] Em resposta ao ofício deste GT5 do CNPD solicitando contribuições.
[84] Disponível em: https://valorinveste.globo.com/produtos/servicos-financeiros/noticia/2021/04/27/34-milhoes-de-brasileiros-ainda-nao-tem-acesso-a-bancos-no-pais.ghtml Acesso em 26/11/2024
[85] Disponível em: https://br.brinks.com/-/brink-s-se-une-%C3%A0-funda%C3%A7%C3%A3o-dom-cabral-em-pesquisa-que-traz-h%C3%A1bitos-e-prefer%C3%AAncias-dos-brasileiros-em-rela%C3%A7%C3%A3o-aos-meios-de-pagamento. Acesso em 26/11/2024

naquele ano. Nesse contexto de déficit informacional, relatório da *Financial Inclusion Global Initiative* (FIGI)[86], aponta que: "A ausência de dados confiáveis sobre crédito e outras informações é um dos principais desafios para ampliar a inclusão financeira. Os dados de telecomunicações podem ajudar a preencher essas lacunas, conectando informações tradicionais de crédito aos dados gerados por consumidores e empreendedores".

11. Ainda, indicador divulgado pelo Banco Mundial considera no cômputo do crédito as operações de financiamento por meio do mercado de capitais. O dado mais recente é de 2022 e mostra que a relação entre o crédito doméstico ao setor privado e a produção interna chegou a 71,8% no Brasil. Esse percentual fica abaixo do observado nos países de renda média, que apresentam uma relação crédito-PIB de 131,6%. Nos Estados Unidos, a relação chegou a 216% em 2022. (ANBC, 2024).

12. No âmbito internacional, o relatório do *World Bank Group (2019)*[87], traz exemplos de como o tratamento de dados pessoais para proteção ao crédito, como o emprego de dados alternativos e algoritmos de pontuação de crédito, são relevantes para o cálculo do *score* de crédito (vide quadro abaixo). Esses métodos permitem maior precisão na análise da capacidade de endividamento, ampliando o acesso ao crédito para indivíduos e setores excluídos[88] e estimulando a economia com maior diversidade de produtos financeiros.

13. Nos últimos anos, o aumento no uso desses mecanismos foi impulsionado pelo acesso a dados, avanços tecnológicos, como aumento do poder computacional e demanda por eficiência[89]. Além de decisões tradicionais sobre concessão de crédito, esses métodos agora abrangem precificação proporcional de serviços, definição de limites, gestão de clientes e segmentação de mercados.

14. Nessa linha de raciocínio, desde a criação das Instituições de Relatórios de Crédito (CRSPs) nos EUA, os dados são essenciais para avaliação de riscos e modelos preditivos[90]. A digitalização ampliou o acesso a dados, permitindo modelos mais precisos, novos produtos e maior inclusão no crédito.

---

[86] Disponível em: https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-DFS-2021-5-PDF-E.pdf. Último acesso em 26.11.2024.
[87] Disponível em: https://thedocs.worldbank.org/en/doc/935891585869698451-0130022020/original/CREDITSCORINGAPPROACHESGUIDELINESFINALWEB.pdf#page=25.15
[88] GPFI (Global Partnership for Financial Inclusion). 2018. G-20 High-Level Principles for Digital Financial Inclusion. https://www.gpfi.org/sites/ gpfi/files/documents/G20%20High%20Level%20 Principles%20for%20Digital%20Financial%20Inclusion%20-%20Full%20version-.pdf.
[89] (Demirguc-Kunt, Klapper e Singer 2017).
[90] CHAPPELL, Gerald et al. The lending revolution: How digital credit is changing banks from the inside. McKinsey & Company) August, at https://www. mckinsey. com/business-functions/risk/our-insights/the-lending-revolution-how-digitalcredit-is-changing-banks-from-the-inside, 2018.

Quadro sobre Tipos de Dados Utilizados para Score de Crédito – *World Bank Group Report*[91]

Categoria de Dados	Tipo de Dados	Aplicação no *Score* de Crédito
Tradicionais	Dados transacionais bancários	Registros de pagamentos atrasados em créditos atuais e passados, valores de empréstimos e histórico de crédito
	Verificações de *bureaus* de crédito	Número de consultas de crédito
	Dados comerciais	Demonstrações financeiras, número de empréstimos para capital de giro, entre outros
Alternativos	Dados de serviços públicos	Registros consistentes de pagamentos pontuais como possível indicador de confiabilidade
	Aplicativos móveis	Sistemas de pagamento móvel com possíveis *insights* sobre o comportamento do consumidor
	Transações *online*	Dados transacionais granulares com possíveis detalhes sobre padrões de gastos
	Dados comportamentais	Psicometria, preenchimento de formulários

15. Como se nota, os instrumentos de proteção ao crédito dependem diretamente do tratamento responsável e lícito de dados pessoais. Esses mecanismos não apenas beneficiam as pessoas naturais e as empresas, oferecendo acesso mais justo, personalizado e controlado ao crédito, mas também fortalecem a economia brasileira, garantindo um ambiente de negócios mais confiável e estimulando o crescimento do país. Dentre eles podemos citar:

- **Cadastro Positivo**: Instituído pela Lei nº 12.414, de 9 de junho de 2011[92], essa lei cria o Cadastro Positivo, uma base de dados que armazena dados sobre o histórico de crédito das pessoas naturais e jurídicas, como pagamentos de contas, empréstimos, financiamentos e cartões de crédito. Ele permite uma avaliação mais ampla e precisa da capacidade de crédito dos indivíduos e empresas ao considerar o comportamento dos devedores diante de obrigações de pagamento e prevê a possibilidade de cancelamento a pedido do cadastrado;

[91] WB GROUP et al. Credit Scoring Approaches Guidelines. The World Bank Group, 2019, pp. 9-13. Disponível em: thedocs.worldbank.org/en/doc/935891585869698451-0130022020/original/CREDITSCORINGAPPROACHESGUIDELINESFINALWEB.pdf#page=25.15

[92] LEI Nº 12.414, DE 9 DE JUNHO DE 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm

- Bancos de Dados como SPC Brasil[93] e Serasa[94]: essas bases coletam informações de inadimplência de devedores e determinam o *score* de crédito de pessoas naturais e empresas, alinhando os créditos concedidos à capacidade de pagamento e prevenindo o superendividamento.

- Agências de proteção ao crédito: como a de enriquecimento cadastral em alto volume da ThinkData[95] que fornecem soluções visando a análise de crédito e o combate à fraude, e que dependem da captura de dados de várias bases de dados, incluindo dados pessoais sensíveis;

- Sistema de Informações de Crédito (SCR)[96]: é um instrumento de registro gerido pelo Banco Central e alimentado mensalmente pelas instituições financeiras. O SCR permite a supervisão bancária a adoção de medidas preventivas, com o aumento da eficácia de avaliação dos riscos inerentes à atividade, e pode evitar o aumento da inadimplência ao disponibilizar um relatório com todas as dívidas contraídas. Através do SCR, o BC consegue verificar operações de crédito atípicas e de alto risco, sempre preservando o sigilo bancário, visando a proteção dos indivíduos e das empresas e gerando um benefício ao país.

3. CONFORMIDADE LEGAL E USO ÉTICO DOS DADOS PESSOAIS, NO BRASIL E EM OUTRAS JURISDIÇÕES

3.1. Abordagens Regulatórias na Tutela do Crédito e sua Aplicabilidade

16. No Brasil, o superendividamento[97] gera uma grande demanda por dados pessoais para controlar riscos de crédito e os prejuízos da inadimplência à economia. A LGPD, inclusive, diferentemente do GDPR, criou uma base legal específica para o tratamento de dados pessoais não sensíveis[98] para a tutela de crédito. A LGPD impõe ainda obrigações de segurança, garantindo proteção contra incidentes de segurança, como acessos não autorizados e vazamentos. Também assegura aos indivíduos inúmeros direitos: de acesso, correção e exclusão de seus dados, além de revisão de decisões automatizadas, aplicáveis no cálculo do risco de crédito.

[93] "O SPC tem soluções para você e para sua empresa". Disponível em: https://www.spcbrasil.org.br/;
[94] Disponível em: https://www.serasa.com.br/
[95] Disponível em: https://www.thinkdata.com.br/produtos/enriquecimento-cadastral-em-alto-volume/
[96] "Sistema de Informações de Créditos (SCR)". Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/scr
[97] "Inadimplência mantém recorde histórico e atinge 68,76 milhões de consumidores, aponta CNDL/SPC Brasil" (18.06.2024). Disponível em: https://site.cndl.org.br/inadimplencia-mantem-recorde-historico-e-atinge-6876-milhoes-de-consumidores-aponta-cndlspc-brasil/
[98] Artigo 7º inciso X da LGPD

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

17. Embora todos os princípios da LGPD devam ser observados em qualquer atividade que envolva tratamento de dados pessoais, no contexto da proteção ao crédito alguns assumem especial relevância, como os princípios da finalidade, da adequação, da transparência, necessidade e o da não discriminação ilícita.

18. O princípio da finalidade, no contexto deste Estudo, deve ser enxergado com o propósito da "proteção ao crédito" para o tratamento de dados pessoais ser legítimo, específico e explícito, tanto é assim que, destacadamente, tutelado na LGPD através de uma base legal própria. Deste modo, é fundamental que os dados tratados para tanto não sejam utilizados de forma desvirtuada, ou seja, é preciso que exista compatibilidade entre o tratamento efetivamente realizado com as finalidades indicadas aos titulares, o que concretiza o princípio da adequação.

19. Nessa linha de ideias, a observância do princípio da transparência é de extrema relevância, sendo imprescindíveis a clareza, a precisão e a facilidade de acesso às informações que são disponibilizadas aos titulares de dados sobre o tratamento de seus dados pessoais para a tutela do crédito.

20. Outro princípio essencial é o da necessidade, que preconiza a limitação do tratamento ao mínimo de dados necessários para a finalidade almejada, evitando excessos ou coleta indiscriminada de informações, devendo ser observado com cautela quando da coleta e tratamento de dados para esse fim.

21. Por fim, o princípio da não discriminação merece também especial atenção, pois as informações tratadas para proteção ao crédito não podem gerar um resultado ilícito ou abusivo.

22. Além da LGPD, a Lei do Cadastro Positivo, como antes mencionado, o CDC e a Lei do Sigilo Bancário também garantem a segurança jurídica no uso de dados para proteção ao crédito.

23. Em acórdão paradigmático do Superior Tribunal de Justiça (STJ), de 12.11.2014, sobre *score* de crédito,[99] decidiu-se que o sistema *credit scoring* é um método desenvolvido para avaliação do risco de concessão de crédito, a partir de modelos estatísticos, considerando diversas variáveis, com atribuição de uma pontuação ao consumidor avaliado (nota do risco de crédito). Na avaliação do risco de crédito, devem ser respeitados os limites estabelecidos pelo sistema de proteção do consumidor no sentido da tutela da privacidade e da máxima transparência nas relações negociais, conforme previsão do CDC e da Lei n. 12.414/2011. De um lado, a metodologia em si de cálculo da nota de risco de crédito (*credit scoring*) constitui segredo da atividade empresarial, cujas fórmulas matemáticas e modelos estatísticos naturalmente não precisam ser divulgadas (art. 5º, IV, da Lei 12.414/2011: ..."resguardado o segredo empresarial"). De outro lado, não se pode exigir o prévio

[99] (STJ- REsp: 1419697 RS 2013/0386285-0, Relator: Ministro PAULO DE TARSO SANSEVERINO, Data de Julgamento: 12/11/2014, S2- SEGUNDA SEÇÃO, Data de Publicação: DJe 17/11/2014 RSSTJ vol. 45 p. 323 RSTJ vol. 236 p. 368 RSTJ vol. 240 p. 256)

e expresso consentimento do consumidor avaliado, pois não constitui um cadastro ou banco de dados, mas um modelo estatístico. Assim, essas informações, quando solicitadas, devem ser prestadas ao consumidor avaliado, com a indicação clara e precisa dos bancos de dados utilizados (histórico de crédito), para que ele possa exercer um controle acerca da veracidade dos dados existentes sobre a sua pessoa, inclusive para poder retificá-los ou melhorar a compreensão do mercado sobre sua capacidade de pagamento.

24. No âmbito internacional, o Regulamento Geral de Proteção de Dados Pessoais (Regulamento (UE) 2016/679 – GDPR) traz diretrizes legais gerais que alcançam a proteção ao crédito, permitindo esse tratamento com base em fundamentos como o legítimo interesse do controlador ou de terceiros, sendo relevante equilibrar a necessidade de avaliar a solvência dos clientes com a proteção dos direitos dos titulares de dados, mediante testes de balanceamento e avaliações de impacto à proteção de dados, além da implementação de medidas de transparência e segurança para garantir a conformidade.

25. De forma mais específica, outras normas de diferentes jurisdições, igualmente vinculantes são aplicáveis a esse contexto:

- Na União Europeia:

26. Diretiva da UE sobre crédito ao consumidor 2023/2225[100]: este documento, destaca a importância da proteção de dados nos contratos de crédito ao consumidor. A Diretiva faz referência explícita ao GDPR, sublinhando sua aplicabilidade ao tratamento de dados pessoais tanto por credores quanto por intermediários de crédito.

[100] Disponível em: https://eur-lex.europa.eu/eli/dir/2023/2225/oj
- Proibição do Uso de Dados Sensíveis (Considerando 48): Credores e intermediários estão proibidos de usar categorias especiais de dados pessoais, como dados de saúde, incluindo informações sobre diagnósticos de câncer.
- Requisitos para Avaliação de Crédito (Considerando 55): A avaliação de crédito deve basear-se em dados necessários, proporcionais, relevantes, precisos e completos, incluindo renda, despesas e obrigações financeiras, mas sem incluir dados sensíveis (ex.: saúde).
- Direito de Revisão em Decisões Automatizadas (Art. 18(8)): Consumidores têm direito a solicitar intervenção humana para obter explicações claras sobre decisões automatizadas, expressar suas opiniões e pedir revisão das decisões relacionadas à avaliação de crédito.
- Bases de Dados e Acesso Não Discriminatório (Art. 19): credores de outros Estados-Membros devem ter acesso igualitário às bases de dados de crédito, desde que em conformidade com o Regulamento (UE) 2016/679. Essas bases devem ser atualizadas e precisas, excluindo dados sensíveis. Consumidores têm direito de contestar informações e devem ser informados sobre mudanças em seus registros.

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

27. Proposta de Regulamento Europeu relativo a *Framework* para acesso a dados financeiros (*Framework for Financial Data Access*)[101]- Parecer do EDPS (*European Data Protection Supervisor*) - *Opinion n. 38/2023*: o objetivo do *Framework* é promover o desenvolvimento de serviços financeiros baseados em dados, permitindo que consumidores e empresas controlem o acesso a seus dados financeiros. Isso facilita o acesso a produtos e serviços personalizados, ao mesmo tempo que mitiga os riscos do compartilhamento de dados. O EDPS analisou a proposta e destacou a importância que o *Framework* dá aos seguintes aspectos relacionados à proteção de dados pessoais: (i) ao controle do cliente sobre os dados [102]; (ii) aos limites de uso de dados[103] seguindo princípios da proporcionalidade e minimização, para evitar discriminação ou exclusão financeira; (iii) necessidade de exclusão de dados sensíveis[104], como informações de saúde ou perfilamento, reduzindo riscos à privacidade; (iv) obrigações dos usuários e Detentores de Dados[105]: usuários devem justificar a solicitação de dados com base legal clara, enquanto detentores de dados garantem precisão, segurança e atualização das informações; (v) cooperação entre autoridades[106]: reguladores financeiros e autoridades de proteção de dados devem trabalhar juntos para evitar conflitos e garantir aplicação coerente das leis; (vi) Diretrizes sobre Uso de[107]: Reguladores como EBA e EIOPA devem estabelecer diretrizes para o uso de dados financeiros em conformidade com leis de proteção de dados, evitando combinações excessivas ou inadequadas.

- Estados Unidos:

28. O sistema americano, liderado pelo setor privado, enfatiza a inclusão financeira e a proteção do consumidor, mas enfrenta desafios relacionados a vieses algorítmicos e falta de transparência. Abaixo, suas principais características:

  - **Dominância do setor privado:** agências como Equifax, Experian e TransUnion lideram o sistema de pontuação de crédito.
  - **Foco na inclusão financeira:** uso de dados alternativos para expandir o acesso ao crédito para populações desbancarizadas e sub-bancarizadas.
  - **Regulamentação para proteger consumidores:** leis como a Lei de Relato Justo de Crédito (FCRA) e a Lei de Igualdade de Oportunidades de Crédito promovem privacidade e práticas justas.

[101] Disponível em: https://www.edps.europa.eu/system/files/2023-08/2023-0730_d2425_opinion_en.pdf#page=8.34
[102] (Recital 2; Art. 8);
[103] (Recital 2; Art. 8 e Recital 18; Art. 7)
[104] (Recital 48; Art. 3):
[105] (Art. 6; Art. 5)
[106] (Art. 18; Art. 26)
[107] Dados (Recital 20; Art. 7)

- **Preocupações com vieses algorítmicos:** apesar das regulamentações, persistem preocupações sobre o potencial de vieses algorítmicos em modelos de ICS devido à falta de transparência;
- **Tensões entre sigilo e transparência:** Conflito entre proteção de segredos comerciais e necessidade de transparência para garantir justiça.
- **FICO Six-Point Test:** a FICO, uma empresa pioneira em pontuação de crédito inovadora nos EUA, desenvolveu um teste rigoroso com critérios para incluir dados em modelos de pontuação, priorizando previsibilidade, conformidade regulatória, relevância, profundidade, abrangência e precisão.

- China:

29. O sistema chinês, impulsionado pelo Estado, prioriza o controle social exacerbado, levantando sérias preocupações sobre a privacidade e o uso indevido de dados. Dentre seus aspectos primordiais, se destacam:

- **Fusão de crédito social e financeiro:** o Sistema de Crédito Social (SCS) avalia credibilidade financeira e "confiabilidade social" com dados de fontes diversas, incluindo plataformas online e instituições financeiras;
- **Participação estatal robusta:** o governo controla o SCS, levantando preocupações sobre privacidade e vigilância intrusiva.
- **Falta de transparência e responsabilidade:** a complexidade e opacidade do SCS dificultam a compreensão de como os dados são usados e protegidos, permitindo ambiguidades e possíveis abusos.
- **Impacto no acesso ao crédito:** baixas pontuações no SCS podem restringir acesso ao crédito e a outros serviços financeiros, ligando comportamento social à capacidade econômica e levantando questões de equidade.
- **Papel das gigantes de tecnologia:** empresas como Alibaba e Tencent são fundamentais no SCS, mas sua proximidade com o Estado gera preocupações sobre privacidade e uso indevido de dados.

30. Estados Unidos x China[108]: Ambos adotaram sistemas de pontuação de crédito inovadores (ICS – *inovative credit scoring*[109]), mas suas abordagens divergem significativamente em termos de atores envolvidos, regulamentação e preocupações com a privacidade – um reflexo de diferentes abordagens e prioridades. Enquanto os EUA optam por uma abordagem mais liberal e voltada ao mercado, a China aposta em uma estrutura centralizada e intervencionista, sendo o tratamento de dados pessoais imprescindível em qualquer contexto.

31. Há, contudo, desafios significativos em ambos os sistemas: nos EUA há uma busca de equilíbrio entre transparência/segredo de negócios e o combate a vieses, e, na China, a grande preocupação ocorre com o grau de proteção dos direitos de liberdade individuais.

32. Tais exemplos servem de parâmetros para análise da situação do Brasil que apresenta uma legislação robusta de proteção de dados pessoais. Ao mesmo tempo em que garante, com a LGPD e outras leis, um tratamento lícito e responsável dos indivíduos e seus dados, permite uma intervenção estatal específica e equilibrada, por meio de órgãos reguladores, para promover a saúde financeira do país.

3.2. Medidas de Governança no Tratamento de Dados Pessoais para Proteção do Crédito

33. A proteção ao crédito, tanto na esfera pública quanto privada, exige que os agentes de tratamento adotem medidas robustas de governança para garantir a conformidade com a legislação de proteção de dados. Agentes, como bancos, financeiras e entidades de registro, têm a responsabilidade de implementar práticas que assegurem a segurança e proteção dos dados pessoais dos titulares. Exemplos adotados por empresas privadas, como Serasa Experian, assim como por entidades oficiais, como o Banco Central, podem ser citados:

- Sistemas e Ferramentas do Sistema Financeiro Nacional e do Banco Central do Brasil ("BACEN" ou "BC"):

    - Relatórios de Impacto à Proteção de Dados Pessoais do BACEN (divulgados publicamente) são um mecanismo legal de tutela dos dados pessoais e servem, ainda, como documento de prestação de

[108] WIJAYA, Trissia; NIDHAL, Muhammad. International experiences with innovative credit scoring: Lessons for Indonesia. Discussion Paper, 2023. Disponível em: https://www.econstor.eu/bitstream/10419/298524/1/1858169704.pdf#page=24.13.

[109] Frequentemente referida como *alternative credit scoring* (ACS) – pontuação alternativa de crédito- nos EUA. Disponível em: https://www.econstor.eu/bitstream/10419/298524/1/1858169704.pdf#page=24.13.

contas com relação à observância da LGPD. Integra a Política de Conformidade do BACEN (PCO - BC)[110];

- Sisbancen: Regulado pela Circular 3.913/2018, é um ecossistema que permite o intercâmbio de informações entre o BC e as instituições supervisionadas. A circular garante a finalidade e o sigilo dos dados enviados ao BC[111].

- Catálogo de Informações do BC: Ferramenta que mantém o registro de todas as bases de dados da instituição, incluindo metadados relevantes para o tratamento e a proteção de dados pessoais.[112]

- Sistema de Transferência de Arquivos do BC (STA): Permite o intercâmbio de arquivos digitais entre o BC e outras instituições, de forma segura e padronizada. [113]

- Rede do Sistema Financeiro Nacional (RSFN): Estrutura de comunicação para o tráfego de informações no Sistema Financeiro Nacional (SFN), utilizada para o envio de dados, inclusive pessoais, com a devida segurança.[114]
    - Sistema Registrado: Permite que os cidadãos consultem seus dados pessoais e financeiros custodiados no BC, garantindo o direito de acesso à informação.
    - Planos de Mitigação de Riscos (PMR): Instrumentos utilizados para planejar e executar ações para reduzir a probabilidade de ocorrência e/ou os impactos dos riscos à proteção de dados pessoais.
    - Sistema *Compliance*: Utilizado para registrar e monitorar as informações de conformidade com a LGPD e outras normas.

- Políticas Internas do BC :

[110] V. RIPD, 2022. Disponível em https://www.bcb.gov.br/content/acessoinformacao/lgpd_docs/relatorio_de_impacto_a_protecao_de_dados_pessoais.pdf
[111] Disponível em: https://www.bcb.gov.br/meubc/sisbacen
[112] Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/seliccatalogodocs
[113] Disponível em: https://www.bcb.gov.br/meubc/sistematransferenciaarquivos
[114] Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/sfn

- Política de Segurança da Informação do BC - PSIBC (Resolução BC 115/2021): Orienta as ações para garantir a segurança da informação, mitigando riscos aos ativos de informação que poderiam comprometer as atividades do BC. A PSIBC é regida pelos seguintes princípios: disponibilidade; integridade; confidencialidade; autenticidade; irretratabilidade; privilégio mínimo; necessidade de conhecer; proteção dos dados pessoais; proteção da privacidade.

- Política de Governança da Informação (PGI-BC) - Portaria 90.187/2016: Define a estrutura de governança da informação do BC, incluindo o Comitê de Governança da Informação (CGI), o Escritório de Governança da Informação (Eginf) e a Auditoria de Observância (AO). A PGI-BC considera a segurança e a privacidade como princípios importantes.

- Política de Privacidade e Termos de Uso do site, dos aplicativos e dos serviços digitais do BC: Define as regras para coleta e uso de dados pessoais em serviços digitais do BC.

- Política de Conformidade do BC (PCO-BC): A PCO-BC tem como objetivo garantir que as atividades do BC sejam conduzidas em conformidade com as normas aplicáveis, incluindo a LGPD.

- Código de Conduta dos Servidores do BC: Define as regras de conduta ética para os servidores do BC, incluindo as diretrizes para o acesso a informações e a proteção de dados pessoais.

- Tabela de Temporalidade do Conselho Nacional de Arquivos (Conarq): Define os prazos para a eliminação de documentos físicos, garantindo que os dados pessoais sejam eliminados de forma segura e em conformidade com a legislação.

- Boas Práticas de *Bureaus* de Crédito – Serasa Experian[115]:

  - Adesão a Padrões Internacionais de Segurança: a Serasa Experian utiliza o *framework* ISO 27001 como base para suas Políticas Globais de Segurança da Informação visando a confidencialidade, integridade e disponibilidade dos dados. Adota também a ISO 27701, uma extensão da ISO 27001, com controles mais específicos de privacidade e proteção de dados, demonstrando a adequação à legislação no que toca à licitude do tratamento e segurança dos dados;

[115] Disponível em: https://www.serasa.com.br/protecao-dados-pessoais/como-protegemos-seus-dados

- Armazenamento Seguro e Gestão de Retenção: os dados são armazenados em ambientes seguros e mantidos pelo tempo necessário para os serviços ou por obrigações legais, com reavaliações periódicas para descartar informações desnecessárias.

- Minimização de Dados: Coleta e trata apenas a quantidade mínima de dados necessários, com processos para definir formatos de dados recebidos e compartilhados.

- Gestão de Fornecedores e Clientes: monitora continuamente fornecedores e clientes visando a conformidade com padrões de proteção de dados e assegurar relacionamentos comerciais confiáveis.

- Avaliação de Impacto e Auditorias Regulares: antes da criação de produtos, o impacto do uso de dados pessoais é avaliado para eliminar possíveis riscos aos consumidores. Auditorias frequentes garantem que os princípios de privacidade e proteção sejam respeitados.

- Transparência e Exercício de Direitos: portal dedicado à proteção de dados pessoais, permitindo que consumidores acessem informações sobre o uso de seus dados, origens, e exerçam seus direitos de maneira clara e atualizada.

- Treinamento Contínuo de Funcionários: colaboradores participam de treinamentos anuais sobre proteção de dados e segurança da informação, reforçando uma cultura organizacional voltada à conformidade.

34. Algumas referências internacionais podem enriquecer exemplos de medidas de governança e boas práticas para tutelar os dados pessoais no contexto de proteção ao crédito e merecem serem citadas:

- Diretrizes para abordagens de pontuação de crédito para os CSPs (*Credit Service Providers)- World Bank Group* [116], nas quais diversos dados pessoais podem ser tratados:

  - Justiça e Não Discriminação: Regulamentos como a Lei de Igualdade de Oportunidades de Crédito (ECOA) nos EUA proíbem discriminação com base em características protegidas, garantindo que as

[116]Disponível em: https://thedocs.worldbank.org/en/doc/935891585869698451-0130022020/original/CREDITSCORINGAPPROACHESGUIDELINESFINALWEB.pdf#page=14.43

metodologias de pontuação de crédito não perpetuem vieses e que as decisões sejam justas e imparciais.

- Requisitos de Capital Regulatório: Acordos como o Acordo de Basileia II exigem que os bancos mantenham capital suficiente para cobrir riscos, incluindo risco de crédito, e que as metodologias de pontuação de crédito sejam adequadas para estimar esses riscos e atender aos requisitos regulatórios.

- Normas Contábeis: As Normas Internacionais de Relato Financeiro (IFRS) exigem que as instituições financeiras reconheçam perdas de crédito esperadas, com as metodologias de pontuação de crédito ajudando a calcular essas perdas e assegurando conformidade com as normas contábeis.

- Governança de Modelos: Reguladores como o *Federal Reserve System*, através da SR 11-7, fornecem diretrizes para a governança de modelos de pontuação de crédito, incluindo validação, monitoramento de desempenho e controles internos, exigindo estruturas robustas de governança para garantir o uso responsável dessas metodologias.

- Autoridade Bancária Europeia (EBA) - Orientações sobre Originação e Monitoramento de Empréstimos [117]

  - Governança Interna e Cultura de Risco de Crédito: As instituições devem adotar uma cultura sólida de risco de crédito, alinhada ao apetite de risco e à estratégia da instituição, assegurando independência entre funções de negócios e risco, treinamento adequado e supervisão das decisões de crédito para garantir responsabilidade e transparência.

  - Processos de Originação de Empréstimos e Monitoramento Contínuo: A avaliação de crédito deve ser baseada em informações precisas sobre a situação financeira do cliente, respeitando a privacidade, com sistemas de monitoramento para revisar créditos e identificar riscos emergentes, mantendo as práticas atualizadas e robustas.

[117] Disponível em: https://www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2020/Guidelines%20on%20loan%20origination%20and%20monitoring/884283/EBA%20GL%202020%2006%20Final%20Report%20on%20GL%20on%20loan%20origination%20and%20monitoring.pdf

- **Uso de Inovações Tecnológicas e ESG:** Modelos automatizados devem ser auditáveis e transparentes, com medidas para prevenir vieses, além de integrar critérios ESG nas políticas de crédito, considerando impactos ambientais e sociais alinhados à sustentabilidade.

- **Transparência, Proteção ao Consumidor e Proporcionalidade:** Políticas devem garantir clareza e equidade, especialmente em decisões automatizadas, evitando práticas que causem superendividamento, com a aplicação proporcional das diretrizes conforme o tamanho e complexidade das instituições e empréstimos, sem prejudicar a proteção ao consumidor.

4. MEIOS PARA AUMENTAR A DISPONIBILIDADE DE DADOS COM RESPONSABILIDADE E SEGURANÇA JURÍDICA

35. Dentre as práticas internacionalmente adotadas para a tutela de dados no contexto de proteção ao crédito, apresentamos ainda as sugeridas pelo *World Bank Group,* abaixo, que focam na ética, transparência e explicabilidade, em modelos de governança, na educação financeira, dentre outros fatores. Tais medidas podem servir de inspiração para melhorar a proteção de dados e garantir a segurança jurídica aos titulares e agentes de tratamento, ao mesmo tempo em que permite o acesso aos dados pessoais necessários para o contexto.

- *World Bank Group* – Diretrizes para abordagens de pontuação de crédito[118]:

  - **Estrutura Legal e Ética:** estabelecimento de um arcabouço legal e ético que assegure o uso responsável de dados pelos CSPs, protegendo direitos fundamentais, privacidade e interesses de consumidores e empresas.

  - **Transparência e Explicabilidade:** decisões de crédito devem ser claras e justas, permitindo que consumidores e reguladores compreendam os critérios usados e acessem mecanismos de contestação.

  - **Responsabilidade no Uso de Dados:** fortalecimento da rastreabilidade, auditorias e cibersegurança para proteger dados contra violações e garantir práticas responsáveis.

  - **Governança de Modelos:** implementação de estruturas para gestão de riscos, testes de desempenho, revisão ética e mitigação de preconceitos nos modelos de crédito.

[118] Disponível em: https://thedocs.worldbank.org/en/doc/935891585869698451-0130022020/original/CREDITSCORINGAPPROACHESGUIDELINESFINALWEB.pdf#page=14.43

- **Colaboração e Compartilhamento de Conhecimento:** promoção de cooperação entre governos, reguladores e o setor privado para fomentar inovação e respeitar a privacidade.

- **Educação Financeira:** incentivo à alfabetização financeira para que consumidores compreendam o uso de seus dados nos modelos de crédito.

- **Equilíbrio entre Inovação e Riscos:** regulamentação que promova inovação em crédito, protegendo dados e garantindo a inclusão financeira sem comprometer privacidade ou ética.

- **Abordagem Regulatória Equilibrada:** proteção contra decisões discriminatórias e uso indevido de dados, conciliando privacidade com desenvolvimento tecnológico e acessibilidade ao crédito.

- **Capacitação de Autoridades e Provedores:** investimento em treinamento e infraestrutura para que reguladores e CSPs acompanhem avanços tecnológicos e apliquem supervisão eficaz.

36. Outra questão relevante é a maior disponibilidade de dados para proteção ao crédito em formato aberto, desde que em conformidade com a legislação. Exemplos federais ilustram esse potencial:

1. **Política de Dados Abertos do Poder Executivo Federal**[119]: Instituída pelo Decreto nº 8.777/2016, promove a transparência, inovação tecnológica e redução de custos, disponibilizando dados acessíveis e reutilizáveis. No contexto de proteção ao crédito, visa garantir acesso a informações confiáveis para análise de crédito, respeitando a LGPD e contribuindo para a governança financeira e desenvolvimento econômico.

2. **Dados Abertos do Sistema Financeiro Nacional**[120]: Liderado pelo Banco Central, disponibiliza informações padronizadas sobre instituições financeiras, taxas e crédito, fomentando transparência, inovação e eficiência no setor. Esses dados estimulam o uso de tecnologia e ciência de dados para o crescimento econômico.

[119] Plano de Dados Abertos do Banco Central do Brasil Maio/2023 – Abril/2025. Disponível em: https://www.bcb.gov.br/content/acessoinformacao/acesso_informacao_docs/Plano_Dados_Abertos_BC_mai2023-abr2025.pdf

[120] Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/dadosabertossfn

37. Assim, seguem os preceitos necessários para o tema do Estudo:

- Finalidade e Proporcionalidade: os dados pessoais devem ser utilizados exclusivamente para finalidades relacionadas à tutela do crédito, observando os princípios da LGPD.

- Transparência e Clareza: titulares de dados têm direito à informação sobre como seus dados são utilizados e podem questionar decisões que os afetem negativamente.

- Inclusão e Não Discriminação: promover acesso equitativo ao crédito, evitando práticas e resultados discriminatórios ilícitos ou abusivos baseadas em dados sensíveis ou inadequados.

  Cibersegurança e Confiança: adotar tecnologias avançadas para proteger dados pessoais e garantir a confiança dos titulares no sistema.

- Legalidade: a prática deve estar alinhada às normas já existentes, como o Código de Defesa do Consumidor, a Lei do Cadastro Positivo e a LGPD.

5. CONCLUSÃO

38. O Estudo de Caso evidencia que a tutela do crédito baseada em dados pessoais é crucial para o crescimento econômico e o bem-estar social no Brasil, ao ampliar o acesso a financiamentos, fomentar o consumo e reduzir riscos de inadimplência. Para a sociedade e indivíduos, promove inclusão financeira com maior acesso a oportunidades, geração de empregos, maior eficiência no sistema de crédito, reduzindo o *spread* bancário,, condições mais justas, proteção contra superendividamento. Quando conduzida de forma ética e transparente, impulsiona a economia sustentável e contribui para a construção de uma sociedade mais justa e inclusiva.

39. Medidas como o fortalecimento da governança de dados, a exemplo da implementação de padrões claros para o uso responsável de informações pessoais e a adoção de mecanismos de segurança condizentes com a legislação de proteção de dados, são fundamentais e fortalecem a segurança jurídica.

40. A integração dessas práticas promove maior confiança no sistema financeiro, facilita o acesso ao crédito e fomenta uma economia mais inclusiva e competitiva.

41. Assim, a Política Nacional de Proteção de Dados Pessoais e Privacidade (PNPD), sob a perspectiva de proteção ao crédito, deveria reconhecer que: (i) o potencial relacionado ao uso de dados pessoais para proteção ao crédito só pode ser plenamente alcançado com respeito aos princípios e preceitos legais estabelecidos pela

LGPD e outras normas aplicáveis, como transparência, finalidade, proporcionalidade, não discriminação ilícita ou abusiva, não utilização de dados sensíveis, segurança, entre outros; (ii) os dados pessoais, quanto mais amplos, qualificados e variados, mais relevantes serão para uma análise de crédito precisa e eficiente, gerando benefícios significativos para a economia e a sociedade, ampliando o acesso ao crédito, reduzindo inadimplências, fomentando a inclusão financeira e impulsionando o desenvolvimento econômico sustentável.

42. Assim, o uso responsável dos dados pessoais deve equilibrar a salvaguarda dos direitos fundamentais de proteção de dados pessoais e privacidade com a maximização de benefícios econômicos e sociais que podem proporcionar.

São Paulo, 18 de dezembro de 2024.

Rony Vainzof
Conselheiro Titular do CNPD

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANEXO XXI – ESTUDO DE CASO: CONTEXTO LABORAL

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

Dados de Função Laboral[121]

I- Introdução

A proteção de dados pessoais no contexto laboral constitui um eixo central das discussões contemporâneas sobre inovação tecnológica, ética corporativa e desenvolvimento econômico sustentável considerando principalmente a assimetria de poder existente nesta relação que decorre do poder diretivo de um lado e do outro a subordinação do trabalhador sendo o contrato de trabalho existencial. Normas internacionais como o GDPR e legislações nacionais, incluindo a LGPD, têm um papel fundamental na regulação desse ambiente, garantindo a proteção dos direitos dos trabalhadores. A Lei Geral de Proteção de Dados (LGPD) estabelece diretrizes que visam não apenas assegurar o tratamento responsável dos dados, mas também equilibrar as prerrogativas dos empregadores e os direitos fundamentais dos trabalhadores, em especial os relacionados à privacidade e à dignidade no âmbito do ambiente de trabalho.

O ambiente laboral, marcado pela crescente digitalização e pelo uso de ferramentas tecnológicas cada dia mais avançadas, tornou-se um espaço privilegiado para a coleta e o tratamento massivo e indiscriminado de dados pessoais. Essas informações, obtidas a partir da relação de trabalho, cumprem finalidades variadas, que incluem desde o recrutamento, gestão de recursos humanos, como o controle de ponto e a concessão de

[121] Este relatório contêm os estudos das especialistas **Caroline de Melo Lima Goularte**. Mestre em Direito pela PUC-RS. Especialista em Compliance pela Faculdade de Direito de Coimbra/Portugal. Profesora convidada nos cursos de pós-graduação em Direito Digital, Proteção de Dados e IA e Advocacia Trabalhista na Escola Brasileira de Direito (EBRADI). Professora convidada em cursos especializados em Compliance e Proteção de Dados Pessoais. Sócia Trabalhista e Head em Compliance e Proteção de Dados no Escritório Denise Fincato Advogados; **Selma Carloto**: Pós-doutora em Direito do Trabalho pela Universidade Federal do Rio Grande do Sul. Doutora em engenharia da informação, Inteligência Artificial pela Universidade Federal do ABC (UFABC). Mestre em Direito pela Universidade São Paulo (USP). Doutorado em Direito do Trabalho pela UBA. Professora autora de Proteção de dados e Compliance Trabalhista da FGV Escola Direito Rio. Professora da FGV de MBA e pós-graduação. Presidente da Comissão de Temporalidade do Instituto Nacional de Proteção de Dados (INPD). DPO certificada pela Exin. DPO e sócia da empresa Madison de implementação de LGPD, Compliance Trabalhista e Canais de Denúncia. Autora do Guia da Associação dos Magistrados do Brasil e da Associação Nacional dos Procuradores do Trabalho "Consentimento como Hipótese Legal de Tratamento". Autora de diversas obras de Lei Geral de Proteção de Dados, Compliance Trabalhista, Inteligência Artificial e ESG e coordenadora e autora de obras de Inteligência Artificial nas Relações de Trabalho e Manual de Relações de Trabalho em Visual Law e **Carlos Carlos Fernandes Coninck Júnior.** Advogado na LBS Advogadas e Advogados. Assessor jurídico da CUT Nacional.

benefícios, até o monitoramento, à análise de desempenho e prevenção de riscos à saúde e segurança ocupacional.

Este documento busca examinar as práticas vigentes, a importância das normas existentes, os desafios e as oportunidades associados ao uso de dados pessoais no âmbito laboral, a partir de estudo de casos, abordando aspectos como hipóteses legais aplicáveis e princípios, negociação coletiva, plataformas digitais, que incluem aspectos relacionados aos impactos da transformação digital e as obrigações das organizações em conformidade com a LGPD. A análise proposta não apenas explora os limites jurídicos e éticos do tratamento de dados no trabalho, mas também propõe soluções para conformidade e garantia dos direitos dos trabalhadores.

II- Normas Internacionais de Proteção de Dados e o Contexto Laboral

1. Regulamento Geral sobre a Proteção de Dados (GDPR)

O GDPR da União Europeia é uma referência global em proteção de dados. O Artigo 88 aborda explicitamente o tratamento de dados no contexto do trabalho, incentivando a regulação desse tema por meio de negociação coletiva. Ele destaca a necessidade de proteger os trabalhadores contra usos abusivos de seus dados, estabelecendo salvaguardas para monitoramento, gestão algorítmica e decisões automatizadas.

1.1 Guidelines

WP29: “Opinion 2/2017 on data processing at work”

Resumo: Este documento do WP29 detalha os princípios aplicáveis ao tratamento de dados no ambiente de trabalho, considerando os avanços tecnológicos, como monitoramento eletrônico e inteligência artificial.

Pontos-chave:

- Consentimento no ambiente laboral: É geralmente inválido, dado o desequilíbrio de poder entre empregador e empregado.
- Proporcionalidade e minimização: O empregador deve garantir que o tratamento de dados seja necessário e limitado ao propósito específico.

- Monitoramento de trabalhadores: Regras rígidas para uso de tecnologias como câmeras, monitoramento de e-mails e rastreamento de localização.
- Revisão de decisões automatizadas: Trabalhadores devem ter o direito de contestar decisões tomadas exclusivamente por algoritmos.

WP29: "Opinion 8/2001 on the processing of personal data in the employment context"

Resumo: Este parecer fornece diretrizes gerais sobre o tratamento de dados em ambientes laborais, sendo uma base para regulamentações posteriores.

Pontos-chave:

- O tratamento de dados deve respeitar a dignidade e a privacidade dos trabalhadores.
- Dados coletados para uma finalidade não podem ser reutilizados para outra, sem justificativa adequada.
- Estímulo à transparência, com comunicação clara aos trabalhadores sobre o uso de seus dados.

EDPB: "Guidelines 05/2020 on consent under Regulation 2016/679"

Resumo: Embora seja uma diretriz geral sobre consentimento no GDPR, aborda o contexto laboral e reforça que o consentimento no trabalho geralmente não é livre.

Pontos-chave:

- O consentimento deve ser utilizado apenas em situações excepcionais no trabalho, quando o trabalhador tiver uma escolha real e livre de coação.
- Alternativas, como "legítimo interesse" ou "execução de contrato", são mais adequadas no contexto laboral.

WP29: "Working Document on the surveillance of electronic communications in the workplace (2002)"

Resumo: Focado no monitoramento de comunicações eletrônicas, como e-mails e acesso à internet no ambiente laboral.

Pontos-chave:

- Os trabalhadores devem ser informados de forma clara sobre as práticas de monitoramento.
- O monitoramento deve ser proporcional e respeitar as finalidades informadas.
- Reitera o direito dos trabalhadores à privacidade, mesmo ao usar dispositivos corporativos.

WP29: "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679" (2018)

Resumo: Estabelece diretrizes sobre decisões automatizadas e criação de perfis, incluindo aquelas aplicadas a trabalhadores.

Pontos-chave:

- Decisões que afetam significativamente os trabalhadores, como promoções ou demissões, não devem ser tomadas exclusivamente por algoritmos, exceto em condições muito específicas.
- Exige explicações claras e revisões humanas para decisões automatizadas.

EDPB: "Guidelines 03/2019 on processing of personal data through video devices"

Resumo: Regula o uso de dispositivos de vídeo, como câmeras de segurança, no ambiente laboral.

Pontos-chave:

- Monitoramento por vídeo deve ser proporcional e minimamente invasivo.
- Locais como banheiros, salas de descanso e vestiários não podem ser monitorados.
- Trabalhadores devem ser informados claramente sobre a presença de câmeras e suas finalidades.

EDPB: "Guidelines on Data Protection Impact Assessment (DPIA)" (2017)

Resumo: Fornece orientações sobre a realização de avaliações de impacto para o tratamento de dados sensíveis, incluindo no trabalho.

Pontos-chave:

- Avaliações de impacto são necessárias quando há monitoramento sistemático de trabalhadores ou uso de tecnologias sensíveis, como biometria.
- Devem incluir consultas com representantes dos trabalhadores ou sindicatos.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

EDPB: “Guidelines 4/2019 on the use of location data and other tracing tools”

Resumo: Focado no uso de dados de localização, que são frequentemente coletados no ambiente laboral por meio de dispositivos GPS ou aplicativos móveis.

Pontos-chave:

- O uso de dados de localização deve ser justificado e comunicado previamente aos trabalhadores.
- O tratamento não pode ser excessivo, e os trabalhadores devem poder desativar o rastreamento fora do horário de trabalho.

WP29: “Opinion on the concept of legitimate interest of the data controller under Article 7 of Directive 95/46/EC”

Resumo: Explora como o “legítimo interesse” pode ser usado como base legal no tratamento de dados laborais.

Pontos-chave:

- O legítimo interesse deve ser equilibrado com os direitos e liberdades fundamentais dos trabalhadores.
- Deve haver uma avaliação rigorosa para evitar abusos.

EDPB: “Guidelines 1/2021 on examples regarding data breach notifications”

Resumo: Embora focado em notificações de violação de dados, inclui exemplos práticos aplicáveis ao ambiente laboral.

Pontos-chave:

- As empresas devem notificar violações que possam expor os dados de trabalhadores a riscos significativos.
- Devem ser implementadas medidas preventivas, especialmente para dados sensíveis, como biometria ou informações financeiras.

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

2. Legislações de Proteção de Dados nos Estados-Membros da União Europeia

2.1. Espanha: Lei Orgânica de Proteção de Dados Pessoais e Garantia de Direitos Digitais (LOPDGDD)

Disposições Laborais:

• Regula o uso de tecnologias de monitoramento no trabalho, como câmeras e sistemas de geolocalização.

• Garante o direito à desconexão digital, protegendo os trabalhadores contra abusos relacionados ao uso de dispositivos fora do horário de trabalho.

2.2. França: Código do Trabalho e a Lei de Proteção de Dados (Loi Informatique et Libertés)

Disposições Laborais:

• O uso de dados de trabalhadores deve ser proporcional e necessário, sendo proibido para finalidades incompatíveis com o contrato de trabalho.

• Conselhos de trabalhadores (Comités Sociaux et Économiques) devem ser consultados antes da implementação de sistemas de monitoramento digital.

2.3. Portugal: Lei n.º 58/2019

Disposições Laborais:

• Estabelece que o empregador só pode tratar dados estritamente necessários à relação de trabalho.

• O Código do Trabalho português proíbe o uso de métodos de vigilância invasivos ou desproporcionais, como gravação de áudio em áreas de descanso.

2.4. Reino Unido: Data Protection Act 2018 (DPA)

• Características: Substitui a legislação anterior após o Brexit, mantendo a conformidade com princípios do GDPR.

Disposições Laborais:

• Exige avaliação de impacto (DPIA) antes da adoção de sistemas de monitoramento no local de trabalho.

• Regulamenta decisões automatizadas envolvendo trabalhadores, garantindo direitos de revisão e explicação.

3. Legislações de Proteção de Dados Fora da União Europeia

3.1. Estados Unidos: Leis Estaduais e Setoriais

• Não há uma lei federal abrangente de proteção de dados, mas leis estaduais e setoriais tocam no tema laboral:

• California Consumer Privacy Act (CCPA): Inclui dados de empregados, permitindo que tenham controle sobre o uso de suas informações.

• Illinois Biometric Information Privacy Act (BIPA): Regula o uso de dados biométricos no trabalho, exigindo consentimento explícito e regras claras de retenção e descarte.

3.2. Canadá: Lei de Proteção de Informações Pessoais e Documentos Eletrônicos (PIPEDA)

• Características: Aplica-se às relações laborais em organizações privadas.

Disposições Laborais:

• Exige que dados sejam tratados apenas para fins legítimos e relevantes à relação de trabalho.

3.3. África do Sul: Protection of Personal Information Act (POPIA)

• Características: Abrange o tratamento de dados em contextos empresariais e laborais.

Disposições Laborais:

• Exige transparência no tratamento de dados, incluindo notificações claras aos trabalhadores sobre finalidades e bases legais.

3.4. Argentina: Ley de Protección de los Datos Personales (Ley 25.326)

• Características: Uma das primeiras legislações na América Latina, regula o uso de dados no trabalho.

Disposições Laborais:

• Estabelece que dados coletados no ambiente de trabalho devem ser usados apenas para fins relacionados à relação laboral.

3.5. China: Personal Information Protection Law (PIPL)

• Características: Regula extensivamente o uso de dados pessoais, com obrigações rigorosas para empregadores.

Disposições Laborais:

• Proíbe o uso de dados pessoais de empregados para monitoramento excessivo.

• Exige consentimento claro e informado para tratamento de dados sensíveis, como biometria.

4. Documentos e Códigos de Trabalho que Regulam Dados Laborais

4.1. Código de Trabalho da Espanha

• Proíbe práticas invasivas de monitoramento que possam violar a dignidade do trabalhador.

• Garante o direito à privacidade em dispositivos eletrônicos fornecidos pelo empregador.

4.2. Código de Trabalho de Portugal

• Proíbe gravações de áudio e vídeo em locais de descanso ou áreas reservadas aos trabalhadores.

• Restringe o uso de vigilância eletrônica para fins estritamente relacionados à segurança.

4.3. Código do Trabalho da França

• Exige que o empregador demonstre a proporcionalidade de qualquer tratamento de dados de trabalhadores.

• Garante o direito de consulta prévia às representações de trabalhadores para adoção de sistemas digitais de monitoramento.

4.4. Leis Trabalhistas no Japão

• Estabelecem que dados pessoais de empregados só podem ser usados com consentimento claro e informado.

• Proíbem a retenção de dados irrelevantes para a relação de trabalho.

5. Convenções da Organização Internacional do Trabalho (OIT)

A OIT reconhece a importância da privacidade e da proteção de dados no ambiente laboral, recomendando que os trabalhadores participem das decisões relacionadas à coleta e ao uso de seus dados.

6. Normas e Diretrizes Internacionais

• Diretrizes da OCDE sobre Privacidade e Fluxos de Dados: Destacam princípios de transparência e minimização de dados no tratamento laboral.

• ISO/IEC 27001: Embora voltada à segurança da informação, aplica-se à proteção de dados sensíveis no trabalho, garantindo práticas seguras e alinhadas às legislações.

III- A LGPD e a Legitimidade no Tratamento de Dados Trabalhistas

A Lei Geral de Proteção de Dados Brasileira (LGPD) afeta as relações de emprego, atingindo a dinâmica da relação entabulada entre empregado e empregador. A incidência das novas obrigações previstas na LGPD exige das organizações uma postura proativa, com vistas à adequação legal.

O Regulamento Europeu de Proteção de Dados prevê, especificamente, o tema da proteção de dados pessoais no âmbito laboral. Conforme o artigo 88 do Regulamento:[122]

> Os Estados-Membros podem estabelecer, no seu ordenamento jurídico ou em convenções coletivas, normas mais específicas para garantir a defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no

[122] UNIÃO EUROPÉIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Bruxelas, 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:32016R0679>. Acesso em: novembro de 2019.

> contexto laboral, nomeadamente para efeitos de recrutamento, execução do contrato de trabalho, incluindo o cumprimento das obrigações previstas no ordenamento jurídico ou em convenções coletivas, de gestão, planeamento e organização do trabalho, de igualdade e diversidade no local de trabalho, de saúde e segurança no trabalho, de proteção dos bens do empregador ou do cliente e para efeitos do exercício e gozo, individual ou coletivo, dos direitos e benefícios relacionados com o emprego, bem como para efeitos de cessação da relação de trabalho.
>
> 2. As normas referidas incluem medidas adequadas e específicas para salvaguardar a dignidade, os interesses legítimos e os direitos fundamentais do titular dos dados, com especial relevo para a transparência do tratamento de dados, a transferência de dados pessoais num grupo empresarial ou num grupo de empresas envolvidas numa atividade económica conjunta e os sistemas de controlo no local de trabalho.

No Brasil, a LGPD não previu, de forma específica, o tema do tratamento de dados pessoais no contexto laboral. Pela leitura do artigo 88 do RGPD, depreende-se que o legislador europeu avança na previsão legal e já direciona às principais preocupações do tratamento de dados pessoais no contexto laboral: a defesa dos direitos e liberdades dos trabalhadores no contexto do tratamento de seus dados pessoais, durante o recrutamento, execução e na cessação do contrato de trabalho; o reconhecimento do princípio da dignidade; a preocupação com a transferência de dados pessoais nos grupos empresariais; e os sistemas de controle no meio ambiente de trabalho.

O direcionamento conferido pelo Regulamento Europeu traz a oportunidade do estudo e adequação à Lei Geral de Proteção de Dados Brasileira (LGPD), no âmbito laboral, com maior segurança jurídica às organizações, haja vista ser o Regulamento Europeu mais exigente, podendo servir de parâmetro para conformação das empresas com o microssistema de proteção de dados.

Conforme já exposto, o tratamento de dados pessoais no âmbito laboral é previsto de forma específica no Regulamento Europeu de Proteção de Dados Pessoais, situação que não foi observada pela Lei Geral de Proteção de Dados Pessoais Brasileira. O artigo 8º da CLT contém as principais técnicas de interpretação e integração da legislação trabalhista. De acordo com Silva[123]:

[123] SILVA, Homero Batista Mateus da. **Comentários à Reforma Trabalhista:** análise da lei 13.467/2017- artigo por artigo. 2 ed. rev. atual. São Paulo: Editora Revista dos Tribunais, 2017, p. 27.

> O legislador de 2017, enfim, manteve intacto o caput do art. 8º e investiu sua energia na elaboração de três parágrafos, voltados, sobretudo, para a censura ao papel que o TST vinha exercendo. O primeiro parágrafo se aproxima muito do anterior, com a única ressalva de que, de certa forma, amplia a aplicação do direito comum: não se exige mais que a aplicação seja feita "naquilo que não for incompatível" com os princípios fundamentais do direito do trabalho. A mudança é quase inócua, porque, de fato, não se pode partir para a aplicação subsidiária em substratos ou contextos diferentes daqueles que norteiam o direito do trabalho, ramo jurídico que lida com relações essencialmente assimétricas. As regras do contrato de compra e venda, por exemplo, jamais poderão balizar as regras do contrato de trabalho porque não guardam nem a mais pálida semelhança [...]

Muito embora o artigo 8º, §1º da CLT[124] preveja que o direito comum é fonte subsidiária do direito do trabalho, o que favorece no preenchimento das lacunas, tendo em vista não ser possível prever todas as hipóteses fáticas que envolvem as relações laborais, compreende-se que a LGPD poderia ter avançado para prever, de forma específica, regras sobre a proteção de dados pessoais nas relações de trabalho (a exemplo do Regulamento Europeu), como forma de conferir maior segurança ao operador jurídico.

IV –Desafios da Proteção de Dados nas Relações de Trabalho

1. O CONSENTIMENTO

No âmbito europeu, parte da doutrina discute que, dada a dependência que resulta da relação empregado/empregador, é pouco provável que o empregado possa negar o seu consentimento ao empregador para o tratamento de seus dados pessoais, sem experimentar o temor e o risco real de efetivos prejuízos, bem como, pouco provável que um empregado possa responder, livremente, a uma solicitação do empregador para

[124] "Art. 8º- As autoridades administrativas e a Justiça do Trabalho, na falta de disposições legais ou contratuais, decidirão, conforme o caso, pela jurisprudência, por analogia, por eqüidade e outros princípios e normas gerais de direito, principalmente do direito do trabalho, e, ainda, de acordo com os usos e costumes, o direito comparado, mas sempre de maneira que nenhum interesse de classe ou particular prevaleça sobre o interesse público. § 1º O direito comum será fonte subsidiária do direito do trabalho." (BRASIL. **Lei 13.467, de 13 de julho de 2017**. Dispõe sobre a alteração da Consolidação das Leis do Trabalho. Brasília, 2017. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13467.htm>. Acesso em: março de 2019).

a coleta de seu consentimento para, por exemplo, ativar sistemas de monitoramento eletrônico, sem se sentir pressionado para tanto.[125]

Nesta senda, suscita-se o argumento de que seria problemático para os empregadores processar dados pessoais dos atuais ou de futuros empregados utilizando a base legal do consentimento, pois, judicialmente, poder-se-ia discutir se a sua outorga foi, efetivamente, livre. Segundo esse entendimento, para a maioria dos tratamentos de dados pessoais de empregados, a base legal, então, não deveria ser o consentimento. Entretanto, não significa que os empregadores nunca possam contar com o consentimento do empregado como base legal para tratamento, pois haverá situações em que a empresa poderá demonstrar que o consentimento, em realidade, deu-se de forma livre.[126]

Para maior segurança na coleta do consentimento do empregado e para que sua utilização seja considerada, efetivamente, válida, faz-se necessário rever cláusulas contratuais, fazer aditivos contratuais, tendo em vista a orientação de que as empresas não podem mais elaborar termos de consentimento muito longos, incompreensíveis, ininteligíveis, devendo constar o propósito (finalidade) do tratamento dos dados pessoais. Nessa linha de raciocínio, o consentimento necessita ser claro, transparente e objetivo.[127]

Para a eficácia do consentimento, em especial nas relações com vínculo empregatício, há diversos documentos que devem ser levados em consideração sempre que as entidades públicas e privadas iniciam os processos de adequação à proteção de dados pessoais.

Dentre os diversos documentos que compõem um sistema de adequação à Lei Geral de Proteção de Dados nas relações de trabalho, o Aviso de Privacidade é voltado para o esclarecimento dos trabalhadores quanto aos seus direitos de privacidade e proteção de dados pessoais, devendo constar as informações de compartilhamento, prazos de armazenamento e eventual descarte, requisitos de licitude para tratamento de seus dados pessoais, sendo imperioso destacar que o Aviso de Privacidade deverá sempre ser lido e interpretado em conjunto com outras políticas e normas internas das organizações, tais como: i) Política de privacidade e proteção de dados; ii) Política de segurança da informação; iii) Política de resposta a incidentes de segurança; iv) Política de atendimento a direitos dos titulares de dados pessoais; v) Política de

[125] UGUINA, Jesús R. Mercader. **Protección de datos y garantia de los derechos digitales en las relaciones laborales**. 3. ed. Madrid: Francis Lefebvre, 2019, p. 42.

[126] UGUINA, Jesús R. Mercader. **Protección de datos y garantia de los derechos digitales en las relaciones laborales**. 3. ed. Madrid: Francis Lefebvre, 2019, p. 42-43.

[127] ARMELIN, Ruth Maria Guerreiro da Fonseca; TEIXEIRA, Tarcisio. **Lei geral de proteção de dados pessoais comentada artigo por artigo**. Salvador: Juspodium, 2019, p. 53.

armazenamento e descarte de dados pessoais. Dentre outros documentos que sejam essenciais para normatizar o tema da proteção de dados pessoais dentro das peculiaridades de cada organização.

Tendo em vista a discussão sobre a utilização do consentimento do empregado como base legal lícita para o tratamento de seus dados pessoais, questiona-se se haveria a possibilidade de negociação coletiva de trabalho suprir o consentimento individual do empregado. A negociação coletiva, enquanto processo democrático de autocomposição de interesses, destina-se à celebração de um instrumento normativo com o objetivo de regular os contratos de trabalho celebrados entre os trabalhadores e os empregadores submetidos aos limites de representação das partes convenentes ou acordantes.[128]

No entanto, o consentimento possui caráter personalíssimo e sua fundamentação reside na possibilidade de autodeterminação do indivíduo em relação aos seus dados pessoais. O consentimento envolve a liberdade de escolha e alinha-se à autodeterminação existencial e informacional do ser humano, revelando-se fundamental para a proteção do indivíduo.[129] Devido ao seu caráter personalíssimo, compreende-se que o consentimento individual do empregado não pode ser suprido por negociação coletiva de trabalho, justo porque o consentimento não tem natureza negocial.[130]

A análise das bases legais que legitimam o tratamento de dados pessoais dos empregados são de extrema importância e aplicabilidade prática para que se evidencie a licitude no tratamento de seus dados pessoais, que ocorrem na fase pré-contratual, durante a relação de emprego e mesmo depois de extinta a relação contratual.

1.1 Consentimento Válido e Transparência

[128] MANUS, Pedro Paulo Teixeira. **Negociação coletiva e contrato individual de trabalho**. São Paulo: Atlas, 2001, p. 109.

[129] TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini. Consentimento e Proteção de Dados Pessoais na LGPD. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords). **Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro.** 1. ed. São Paulo: Thompson Reuters Brasil, 2019, p. 287-320, p. 299.

[130] É inadequado atribuir a natureza negocial, pois isto significaria dizer que há um sinalagma entre o consentimento para o tratamento de dados pessoais e determinada vantagem econômica obtida por quem consente, o que reforçaria a natureza contratual e de incentivo ao uso dos dados pessoais como direito patrimonial e não personalíssimo. Nesse sentido, conforme Doneda: "O consentimento para tratamento de dados pessoais toca diretamente elementos da própria personalidade, porém não dispõe desses elementos. Ele assume mais propriamente as vestes de um ato unilateral, cujo efeito é o de autorizar um determinado tratamento para os dados pessoais, sem estar diretamente vinculado a uma estrutura contratual." (DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro, 2006, p. 377-378).

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

- Estudo de Caso 1

Consentimento Forçado e Desrespeito a Princípios no Recrutamento e Seleção

O processo de recrutamento e seleção apresenta desafios específicos relacionados ao tratamento de dados pessoais. É comum que empresas adotem práticas inadequadas, como o consentimento forçado e genérico, o que resulta na nulidade desse consentimento nos termos da Lei Geral de Proteção de Dados (LGPD). Essa prática não apenas viola o artigo 8º da LGPD, mas também prejudica os direitos dos titulares, principalmente artigo 18, incisos VI, VIII e IX.

Outro problema frequente é a coleta excessiva de dados no contexto das relações de trabalho, em desacordo com os princípios fundamentais da LGPD, como os de **necessidade** e **finalidade**. Além disso, muitas empresas tratam dados pessoais sem qualquer transparência, omitindo informações sobre o tratamento e falhando em fornecer avisos de privacidade adequados.

Este estudo de caso examina as medidas necessárias para corrigir essas falhas, assegurando a conformidade com a legislação e promovendo o respeito aos direitos dos titulares. O objetivo é proporcionar um modelo de boas práticas, que alie a proteção de dados ao sucesso das estratégias de recrutamento e seleção.

Ao compreender os desafios no tratamento de dados pessoais em processos de recrutamento e seleção, torna-se essencial abordar práticas específicas que frequentemente desrespeitam a LGPD. Um exemplo comum é o uso inadequado do consentimento forçado em plataformas de recrutamento, prática detalhada a seguir.

Consentimento Forçado em Plataformas de Recrutamento:

É muito comum, e esse erro vem sendo amplamente replicado, que plataformas de recrutamento agrupem diversas finalidades de tratamento sob um único consentimento genérico. Essa prática, no entanto, contraria as exigências legais, pois para que o consentimento seja válido, ele deve ser granular, ou seja, vinculado a finalidades específicas e determinadas, conforme o disposto no **art. 8º, §4º, da Lei Geral de Proteção de Dados (LGPD)**.

O consentimento válido exige uma manifestação livre, informada e inequívoca do titular, nos termos do **art. 5º, inciso XII, da LGPD**, que o define como: *"manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada."* Essa granularidade é essencial

para garantir que o titular tenha pleno controle sobre seus dados e que o tratamento esteja alinhado aos princípios da legislação, promovendo transparência e respeito aos direitos fundamentais. [131]

Por essa razão, é fundamental que as plataformas de recrutamento e as empresas adotem práticas de consentimento que respeitem a granularidade exigida pela LGPD, quando esta for a hipótese legal de tratamento. Isso significa apresentar ao titular opções claras e separadas para cada finalidade de tratamento, garantindo que ele tenha plena liberdade para autorizar apenas os tratamentos que considerar adequados. Além disso, é comum que essas plataformas utilizem o consentimento como hipótese legal para diversas finalidades, mesmo quando deveriam se enquadrar em outras hipóteses legais de tratamento previstas na LGPD. Essa prática, além de desnecessária, pode prejudicar a transparência e a proteção dos direitos dos titulares.

Para ilustrar como essas práticas inadequadas se manifestam, apresentamos um exemplo prático que evidencia a desconformidade com a LGPD e demonstra como o consentimento genérico pode comprometer os direitos dos titulares.

Como não pode ser:

☐ Aceito a Política de Privacidade para que meus dados sejam processados para esta vaga e futuros processos seletivos que se enquadrem em meu perfil, bem como para receber comunicações por meio dos canais disponíveis, incluindo o WhatsApp.

Por quê?

[131] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Redação dada pela Lei nº 13.853, de 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 23 nov. 2024.

Se o consentimento fosse a hipótese legal de tratamento, não poderia ser genérico para várias finalidades, mas deveria ser granular. Nesse exemplo, o consentimento agrupa três finalidades distintas:

1. Tratamento de dados para a vaga atual.
2. Tratamento de dados para futuros processos seletivos.
3. Envio de comunicações por diversos canais, incluindo o WhatsApp.

Quando o consentimento for a hipótese legal de tratamento, ele deve ser **granular**, ou seja, coletado separadamente para cada finalidade específica, conforme determina a **Lei Geral de Proteção de Dados (LGPD)**.

Diante de práticas inadequadas, é essencial propor alternativas que respeitem a LGPD e garantam a conformidade. A seguir, sugerimos um exemplo de como as empresas podem estruturar o consentimento de forma adequada e alinhada à legislação.

Sugestão de como poderia ser em conformidade com a LGPD:

> A Empresa "X" respeita a privacidade e a proteção de seus dados pessoais, cumprindo integralmente as disposições da Lei Geral de Proteção de Dados (LGPD). Para mais detalhes sobre o tratamento dos seus dados, consulte nosso Aviso de Privacidade (link de acesso ao aviso de privacidade).
>
> Confira abaixo as finalidades e hipóteses legais para o tratamento de seus dados pessoais neste processo seletivo e no banco de talentos:
>
> **Este processo seletivo:** o tratamento de dados pessoais é realizado com fundamento no art. 7º, inciso V da LGPD, quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual você seja parte.
>
> **Banco de Talentos:** além disso, utilizamos o legítimo interesse como hipótese legal, nos termos do art. 7º, inciso IX da LGPD, para manter suas informações em nosso banco de talentos por até 1 (um) ano, com o objetivo de analisar futuras oportunidades de emprego que se adequem ao seu perfil. Você tem o direito de exercer o direito de oposição (*opt-out*) ao tratamento posterior de seus dados, fora da finalidade inicialmente solicitada, a qualquer momento. Caso

não deseje que suas informações sejam mantidas para este fim, pode solicitar a exclusão de seus dados do nosso banco de talentos.

Envio de comunicações:

Enviamos apenas mensagens referentes aos processos seletivos atuais nos quais você se inscreveu e, para futuros processos seletivos, somente se você não tiver se oposto ao tratamento de suas informações.

Para mensagens com fins **não relacionados** a oportunidades de trabalho, como conteúdos promocionais, publicitários ou convites para eventos institucionais, o envio será realizado apenas mediante sua autorização.

☐ **Autorizo** o envio de mensagens com fins não relacionados a oportunidades de trabalho, como conteúdos promocionais, publicitários ou convites para eventos institucionais.

☐ **Não autorizo** o envio de mensagens com fins não relacionados a oportunidades de trabalho.

Com base nos princípios e sugestões apresentados a partir de pesquisa empírica em plataformas de recrutamento e seleção, analisamos um caso real que exemplifica a desconformidade de consentimento em plataformas de recrutamento. A descrição do caso reforça a necessidade de adequação às exigências da LGPD.

- Estudo do Caso 2

Uma plataforma de recrutamento exige que os candidatos aceitem a política ou aviso de privacidade (com nomenclatura variável entre empresas) como condição para seguir no processo seletivo. Essa aceitação abrange diversas finalidades, como análise de perfil para a vaga pretendida, inclusão em banco de talentos e envio de comunicações futuras relacionadas e não relacionadas ao processo de recrutamento e seleção, sem permitir granularidade ou escolha seletiva. Caso o candidato não aceite, não é possível prosseguir no cadastro.

Análise de Conformidade:

- Hipótese legal Inadequada:

O consentimento generalizado para todas as finalidades é incorreto. Para a análise de perfil no processo seletivo, a hipótese legal adequada seria **procedimentos preliminares para a execução de contrato** (art. 7º, V da LGPD).

Já para inclusão em banco de talentos a hipótese legal de tratamento mais adequada é o legítimo interesse, o que exige um teste de balanceamento e para o envio de comunicações futuras, **que não se relacionem com o processo de recrutamento,** deve-se utilizar o **consentimento granular**.

- **Prática de Consentimento Forçado:**

Forçar o consentimento **viola o artigo 8º e os direitos do titular, artigo 18**, **incisos VIII e IX**, que asseguram liberdade de escolha, consentimento para finalidades específicas e a possibilidade de revogação do consentimento.

- **Falta de Transparência:**

A ausência de informações claras em um aviso ou política de privacidade detalhada sobre cada finalidade de tratamento também contraria os princípios da transparência (art. 6º, VI da LGPD), assim como o da finalidade e o artigo 9o. da LGPD.

Solução Proposta:

Para garantir a conformidade com a LGPD, a plataforma deve adotar as seguintes medidas:

- **Como Escolher as Hipóteses Legais de Tratamento Adequadas:**

Quando o tratamento de dados for indispensável e solicitado diretamente pelo titular ao utilizar a plataforma, a hipótese legal aplicável deve ser a **execução de contrato ou procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados, conforme previsto no art. 7º, V da LGPD,** eliminando a necessidade de consentimento. Para tratamentos adicionais baseados em uma situação concreta e vinculados a uma finalidade legítima, específica e explícita, é possível fundamentar o tratamento no **legítimo interesse do controlador**, desde que seja respeitado o disposto no art. 10 da LGPD, garantindo que:

- A finalidade do tratamento seja legítima e relacionada às atividades do controlador ou à proteção de direitos do titular.
- Apenas os dados estritamente necessários à finalidade pretendida sejam tratados (§ 1º, art. 10).
- A transparência seja assegurada por meio de medidas claras, como aviso de privacidade adequado, que informe os titulares sobre o tratamento, suas medidas de salvaguarda e a possibilidade de exercício de direitos, como oposição ou “opt-out”(§ 2º, art. 10).

Para finalidades assessorias, que dependam de consentimento, como o envio de comunicações **não** referentes ao processo seletivo por canais como WhatsApp, este deverá ser granular, o que permite ao titular selecionar quais finalidades autoriza.

Quando o consentimento for a hipótese legal de tratamento, oferecer ao titular opções claras, como **"Autorizo"** e **"Não autorizo"**, **"Aceito"** ou **"Não aceito"**, ou ainda permitir que o titular marque um campo com **"X"** para autorizar o tratamento. A manifestação deve ser livre, inequívoca e de acordo com o art. 8º da LGPD.

Hipóteses Legais de Tratamento no caso estudado

No caso analisado, considerando o exemplo de como "**não deve ser" e "como pode ser",** foram apresentadas **três finalidades de tratamento** agrupadas de forma inadequada. Cada finalidade deve ser tratada individualmente, podendo, em alguns casos, ter a mesma hipótese legal.

Para o caso em questão, as hipóteses legais de tratamento seriam:

Processamento de dados para esta vaga:

Hipótese Legal: procedimentos preliminares relacionados à execução de contrato a pedido do titular, conforme o **art. 7º, inciso V, da LGPD**.

Processamento de dados para futuros processos seletivos que se enquadrem no perfil do candidato:

Hipótese Legal: legítimo interesse do controlador, nos termos do **art. 7º, inciso IX, da LGPD**, para manter os dados em um banco de talentos. Essa prática exige análise de balanceamento para preservar os direitos do titular, com informações claras sobre a finalidade, prazo de armazenamento e possibilidade de oposição (opt-out) a qualquer momento.

Envio de mensagens a candidatos

O envio de mensagens para candidatos pode se basear nas seguintes hipóteses legais de tratamento previstas pela **Lei Geral de Proteção de Dados (LGPD)**, dependendo do contexto e da finalidade da comunicação:

Execução de Contrato ou Procedimentos Preliminares Relacionados a Ele (Art. 7º, V)

Se a mensagem for relacionada a processos seletivos ou etapas para a formalização de um contrato de trabalho (como entrevistas, entrega de documentos ou feedback), é possível enquadrar o envio como necessário para atender aos procedimentos preliminares a um contrato.

Legítimo Interesse do Controlador (Art. 7º, IX)

Caso as mensagens sejam para fins relacionados ao andamento do processo seletivo, comunicação de vagas futuras ou manutenção do relacionamento com o candidato para oportunidades futuras, o legítimo interesse pode ser utilizado. Nesse caso, é essencial realizar um teste de balanceamento (LIA) para demonstrar que o envio não viola os direitos e liberdades dos titulares.

Consentimento (Art. 7º, I)

Se as mensagens tiverem finalidades que excedam o processo seletivo, como envio de materiais promocionais ou campanhas, deve ser previamente obtido o consentimento do candidato.

Considerações Adicionais

Transparência

É fundamental garantir que o aviso de privacidade informe, de forma clara e acessível as hipóteses legais aplicáveis ao tratamento de dados pessoais. Essas informações devem estar alinhadas aos princípios da LGPD, promovendo a confiança e o entendimento por parte do titular.

Direito de Oposição (Opt-out)

O candidato deve ter a possibilidade de recusar ou interromper o recebimento de mensagens que não sejam essenciais ao processo seletivo. Para tratamentos que dependam de consentimento ou estejam fundamentados no legítimo interesse, é necessário assegurar um mecanismo simples e eficaz para exercer o direito de oposição e o de revogação respectivamente.

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

Aviso de Privacidade

O aviso de privacidade deve detalhar, de forma clara e objetiva:

- Todas as hipóteses legais que fundamentam o tratamento de dados pessoais.
- As finalidades específicas e legítimas para cada tipo de tratamento.
- A garantia de que os dados serão tratados exclusivamente para os fins informados.

Participação no Processo Seletivo

É imprescindível que o candidato possa participar integralmente do processo seletivo sem ser obrigado a aceitar finalidades acessórias, como o envio de comunicações não relacionadas diretamente à seleção. Para tratamentos que dependam de consentimento, o aviso de privacidade deve informar claramente:

- Que o candidato tem a liberdade de recusar essas finalidades adicionais.
- Que a recusa não afetará sua participação no processo seletivo.

Respeito às Finalidades Dependentes de Consentimento

Quando o tratamento estiver vinculado ao consentimento, é necessário assegurar que:

- O titular possa decidir livremente sobre estas finalidades adicionais.
- A inscrição no processo seletivo seja atendida mesmo que o candidato opte por não autorizar o uso de seus dados para outras finalidades, como comunicações de marketing ou similares.

O respeito às finalidades dependentes de consentimento não apenas reforça os direitos dos titulares, mas também estabelece práticas de conformidade que evitam a aplicação de consentimento genérico ou compulsório. No entanto, essas práticas inadequadas não se limitam ao contexto de recrutamento e seleção. Situações semelhantes podem ser observadas em outros setores, como exemplificado no Guia da ANPD do Poder Público. A seguir, analisamos um caso relacionado ao consentimento inadequado no contexto de matrícula de estudantes em universidades públicas, que apresenta paralelos relevantes e lições aplicáveis ao recrutamento.

Comparação com e exemplo similar em outro contexto no guia da ANPD do Poder Público: “Matrícula de Estudante em Universidade Pública”

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

O Guia da Autoridade Nacional de Proteção de Dados (ANPD) do Poder Público, na página 12, apresenta um exemplo de consentimento inadequado no contexto de universidades públicas:

Estudantes são obrigados a fornecer dados pessoais para cadastro e matrícula online. O procedimento exige que, para prosseguir com a escolha de disciplinas e horários, o estudante "aceite" condições de tratamento descritas de forma genérica, com menções vagas como *"fins educacionais e outros correlatos"*. Além disso, a recusa ao consentimento impede a matrícula e o acesso a serviços essenciais, como assistência estudantil e biblioteca.

Segundo a ANPD, esse consentimento seria considerado inválido pelos seguintes motivos:

1. Os titulares não têm condições de recusar o tratamento de seus dados, dado o caráter compulsório da operação.
2. Estão sendo levados a autorizar um tratamento com finalidades genéricas, sem clareza ou precisão.

Para adequação à LGPD, o Guia orienta que a universidade forneça informações específicas sobre as finalidades do tratamento e identifique uma hipótese legal mais apropriada, como o cumprimento de obrigação legal ou regulatória. Além disso, deve ser garantido que apenas dados estritamente necessários sejam coletados, respeitando o princípio da necessidade.

O exemplo apresenta desconformidade similar ao Contexto de Recrutamento:

Situação similar ao exemplo apresentado no Guia da ANPD ocorre no cenário de recrutamento e seleção, conforme ilustrado a seguir:

☐ Aceito a Política de Privacidade para que meus dados sejam processados para esta vaga e futuros processos seletivos que se enquadrem em meu perfil, bem como para receber comunicações por meio dos canais disponíveis, incluindo o WhatsApp.

Essa prática apresenta as seguintes inconsistências, semelhantes às identificadas pela ANPD:

1. Consentimento Compulsório: o consentimento é exigido de forma obrigatória para que o candidato prossiga no processo seletivo ou utilize a plataforma, o que elimina a liberdade de escolha.
2. Finalidades Amplas e Genéricas: as finalidades abrangem desde a candidatura a uma vaga específica até a inclusão em banco de talentos e o envio de comunicações, sem especificidade ou granularidade.

Recomendações para Adequação

A empresa controladora ou a plataforma de recrutamento deve:

1. Informar claramente as finalidades específicas de cada tratamento de dados.
2. Evitar vincular consentimento compulsório ao acesso ao serviço, utilizando outras hipóteses legais apropriadas, como:

Procedimentos preliminares para a execução do contrato (Art. 7º, V, LGPD) para a vaga específica.

Legítimo interesse (Art. 7º, IX, LGPD) para manter dados em um banco de talentos, assegurando o direito de oposição e respeitando os princípios de necessidade e transparência.

3. Garantir que o consentimento, quando utilizado, seja granular e facultativo, permitindo ao titular escolher quais finalidades autoriza.

- Estudo de Caso 3: Gerenciamento de Banco de Talentos

Descrição do Caso

Após o término de um processo seletivo, os currículos de candidatos não aprovados são mantidos em um banco de talentos. Alternativamente, a empresa disponibiliza um cadastro voluntário para candidatos interessados em futuras vagas, sem estarem vinculados a um processo específico.

Análise de Conformidade

Distinção de Hipóteses Legais:

1-No caso de currículos mantidos após um processo seletivo, a hipótese legal é o **legítimo interesse** (Art. 7º, IX da LGPD).

2- Para cadastros voluntários, **quando o titular busca o tratamento**, aplica-se execução de contrato ou de **procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados** (Art. 7º, V da LGPD).

Solução Proposta

- Criar um aviso de privacidade com informações claras sobre cada finalidade e hipóteses legais de tratamento, além de compartilhamentos, prazos de retenção claros, canal de contato e identificação da identidade do DPO.
- Oferecer direito de oposição *(opt-out)* para titulares, garantindo sua autonomia no uso dos dados.

Aviso de Privacidade

Abaixo, um modelo de Aviso de Privacidade para empresas de recrutamento:

Aviso de Privacidade – Recrutamento e Seleção
A (nome da empresa) valoriza a privacidade e proteção de dados pessoais, cumprindo a LGPD.

- ✓ Dados coletados: nome completo, contato, qualificação e experiência profissional.
- ✓ Finalidades e hipóteses legais de tratamento

  Participação em processos seletivos atuais: art. 7º, V, procedimentos preliminares para execução de contrato.
  Inclusão no banco de talentos para análise em vagas futuras: art. 7º, IX, legítimo interesse
  Envio de comunicações, incluindo oportunidades de emprego e materiais informativos: art. 7o. ,I, consentimento livre, informado e inequívoco

- ✓ Retenção de dados: até 1 ano em banco de talentos, com exclusão automática após este período ou quando exercido o direito de oposição pelo titular.
- ✓ Direitos do titular: você pode solicitar a exclusão de seus dados a qualquer momento enviando um e-mail para (contato).
- ✓ Compartilhamentos: seus dados poderão ser compartilhados com:

  Empresas contratantes em processos seletivos nos quais você estiver inscrito.

  Parceiros tecnológicos responsáveis pelo armazenamento e gerenciamento de dados.
- ✓ Canal de contato: para dúvidas ou solicitações relacionadas à privacidade de seus dados, envie um e-mail para (...).

Outro exemplo diferente de desconformidade encontrado em portais de recrutamento:

☐ Aceito as Condições Legais e a Política de Privacidade da empresa X para criar uma conta no portal, participar de processos seletivos, estabelecer contato com empregadores e receber comunicações do XXXX por WhatsApp ou outros meios.

Hipóteses legais de tratamento adequadas:

Criar uma conta no portal

- Hipótese legal: procedimentos preliminares para execução de contrato (art. 7º, V, LGPD).
- Justificativa: o cadastro é necessário para permitir o acesso aos serviços oferecidos pelo portal.

Candidatar-me a vagas de emprego

- Hipótese legal: procedimentos preliminares para execução de contrato (art. 7º, V, LGPD).
- Justificativa: o tratamento de dados é essencial para viabilizar o envio de candidaturas a vagas específicas.

Entrar em contato com possíveis empregadores

- Hipótese legal: procedimentos preliminares para execução de contrato (art. 7º, V, LGPD).
- Justificativa: os dados são utilizados para viabilizar a comunicação entre o candidato e o empregador no âmbito do processo seletivo.

Receber comunicações do portal via WhatsApp ou outros meios

- Hipótese legal: consentimento livre, informado e inequívoco (art. 7º, I, LGPD).
- Justificativa: o envio de comunicações, incluindo informações de marketing ou atualizações, exige consentimento do titular, pois vai além das finalidades essenciais do serviço.

2.DECISÕES AUTOMATIZADAS

Interessante ponderação deve ser feita quanto à responsabilidade empresarial no uso da inteligência artificial. As técnicas de privacidade desde a concepção (*privacy by design*) e por padrão (*privacy by default*) dos produtos ou serviços, bem como a implementação de um sistema de *compliance* trabalhista digital podem auxiliar na orientação dos empresários na utilização desses sistemas.

A digitalização ocasiona transformações desafiadoras no meio ambiente de trabalho. A tomada de decisões laborais automatizadas, como é o caso da utilização de programas informáticos que recrutam e selecionam candidatos a emprego, não possui regramento específico no ordenamento jurídico brasileiro. É possível, pela interpretação do artigo 8º, § 1º da CLT, que o direito comum seja fonte subsidiária do Direito do Trabalho, pela impossibilidade de se prever todas as hipóteses fáticas que envolvem as relações laborais.

Entretanto, nem a Lei Geral Brasileira de Proteção de Dados, nem o Regulamento Europeu de Proteção de Dados respondem, eficientemente, a este questionamento: qual a responsabilidade do empregador diante do uso da inteligência artificial no meio ambiente de trabalho, especificamente, neste caso, qual seria a responsabilidade do empregador diante do uso de inteligência artificial no recrutamento e seleção de empregados?

O artigo 88 do Regulamento Europeu de Proteção de Dados prevê que os Estados-Membros podem estabelecer, no seu ordenamento jurídico ou em convenções coletivas, normas mais específicas para garantir direitos e liberdades sobre o tratamento de dados pessoais dos trabalhadores.[132]

---

[132] "Artigo 88. Tratamento no contexto laboral. 1. Os Estados-Membros podem estabelecer, no seu ordenamento jurídico ou em convenções coletivas, normas mais específicas para garantir a defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no contexto laboral, nomeadamente para efeitos de recrutamento, execução do contrato de trabalho, incluindo o cumprimento das obrigações previstas no ordenamento jurídico ou em convenções coletivas, de gestão, planeamento e organização do trabalho, de igualdade e diversidade no local de trabalho, de saúde e segurança no trabalho, de proteção dos bens do empregador ou do cliente e para efeitos do exercício e gozo, individual ou coletivo, dos direitos e benefícios relacionados com o emprego, bem como para efeitos de cessação da relação de trabalho. 2. As normas referidas incluem medidas adequadas e específicas para salvaguardar a dignidade, os interesses legítimos e os direitos fundamentais do titular dos dados, com especial relevo para a transparência do tratamento de dados, a transferência de dados pessoais num grupo empresarial ou num grupo de empresas envolvidas numa atividade económica conjunta e os sistemas de controlo no local de trabalho. 3. Os Estados-Membros notificam a Comissão das disposições de direito interno que adotarem nos termos do n. 1, até 25 de maio de 2018 e, sem demora, de qualquer alteração subsequente das mesmas." (UNIÃO EUROPÉIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao

O artigo 22 do mesmo Regulamento dispõe sobre as decisões individuais automatizadas, incluindo a definição de perfis. Referido artigo prevê que o titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada, exclusivamente, com base no tratamento automatizado, que produza efeitos na sua esfera jurídica, ou que o afete, significativamente, de forma similar. As alíneas "a" e "c" do item 2 do artigo 22 fazem a ressalva no sentido de ser possível que o titular dos dados fique sujeito a uma decisão tomada, exclusivamente, com base em tratamento automatizado, desde que seja necessário para execução de um contrato entre o titular dos dados e um responsável pelo tratamento, e no caso do tratamento ser baseado no consentimento explícito do titular dos dados.[133]

A Lei Geral de Proteção de Dados dispõe, no artigo 20, que o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil profissional. O §1º do artigo 20 prevê que o controlador (que, no tratamento de dados pessoais em uma relação de emprego poderá ser o empregador), deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

---

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). Bruxelas, 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:32016R0679>. Acesso em: novembro de 2019).

[133] "Artigo 22. Decisões individuais automatizadas, incluindo definição de perfis. 1. O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar. 2. O n. 1 não se aplica se a decisão: a) For necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento; b) For autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou c) For baseada no consentimento explícito do titular dos dados. 3. Nos casos a que se referem o n. 2, alíneas a) e c), o responsável pelo tratamento aplica medidas adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados, designadamente o direito de, pelo menos, obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão. 4. As decisões a que se refere o n. 2 não se baseiam nas categorias especiais de dados pessoais a que se refere o artigo 9, n. 1, a não ser que o n. 2, alínea a) ou g), do mesmo artigo sejam aplicáveis e sejam aplicadas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular." (UNIÃO EUROPÉIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Bruxelas, 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:32016R0679>. Acesso em: novembro de 2019).

No § 2º do artigo 20 há a disposição clara de que no caso do não fornecimento das informações solicitadas, a autoridade nacional poderá realizar auditoria para verificar aspectos discriminatórios no tratamento automatizado de dados pessoais.[134]

É oportuno esclarecer a diferença entre os termos automação e automatização. O primeiro diz respeito a substituição de tarefas manuais por processos que operam automaticamente, sem necessariamente envolver sistemas complexos ou inteligência artificial, enquanto a automatização envolve um processo mais complexo com a utilização de tecnologias mais avançadas, como a inteligência artificial, aprendizado de máquina e algorítmicos sofisticados, incluindo a tomada de decisões baseadas em análise de dados e padrões identificados por sistemas. O artigo 20 da LGPD trata, especificamente, de processos automatizados, no sentido mais amplo e avançado, os quais podem impactar significativamente a vida do titular de dados.

Importa referir que a LGPD foi alterada pela lei nº 13.853/2019. Antes dessa alteração legislativa, a LGPD previa no *caput* do artigo 20 que o titular dos dados teria o direito a solicitar revisão, por pessoa natural, das decisões tomadas com base em tratamento automatizado. Entretanto, a alteração legislativa retirou a expressão "por pessoa natural", levando a conclusão de que, no Brasil, as decisões tomadas com base em tratamento automatizado poderão ser revistas, também, de forma automatizada, e não necessariamente por pessoa natural.

A falta de um melhor direcionamento legal sobre esta temática (inclusive porque o legislador não consegue acompanhar a velocidade da tecnologia, que avança de forma desmedida), fez com que um grupo de especialistas de alto nível da União Europeia, criado pela Comissão Europeia, elaborasse um documento intitulado "Orientações Éticas para uma IA de Confiança". Nesta declaração, que é direcionada à Europa, a

[134] "Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (Redação dada pela Lei nº 13.853, de 2019). § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial. § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais." (BRASIL. **Lei 13.709, de 14 de agosto de 2018.** Dispõe sobre a Lei Geral de Proteção de Dados Pessoais. Brasília, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: novembro de 2019).

intenção é lançar luzes aos necessários valores e princípios fundamentais para um modelo de convivência democrática e de cidadania, com respeito aos direitos humanos, à democracia e ao Estado de Direito.[135]

Dentre os princípios éticos constantes nesse documento, para fins deste trabalho, ressalta-se o princípio da "explicabilidade", que prevê que os processos operados com inteligência artificial necessitam ser transparentes e as decisões automatizadas devem ter a possibilidade de serem explicadas aos titulares dos dados; e o princípio da "prevenção de enviesamentos injustos", ao dispor que os dados utilizados pelos sistemas de inteligência artificial podem ser afetados pela inclusão de desvios históricos inadvertidos e que a manutenção de tais desvios pode dar origem à discriminação e preconceitos. Essa declaração orienta que o enviesamento discriminatório deve ser eliminado na fase de coleta de dados, sempre que possível, devendo ser combatido mediante a adoção de processos de supervisão para analisar e abordar a finalidade, os condicionalismos, os requisitos e as decisões do sistema de forma clara e transparente.[136]

---

[135] HIGH-LEVEL EXPERT GROUP ON AI (AI HLEG). **Ethics Guidelines for Trustworthy AI.** Bruxelas: European Commission, 2019. Disponível em: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>. Acesso em: junho de 2019.

[136] "*Explicabilidade*. A explicabilidade diz respeito à capacidade de explicar tanto os processos técnicos de um sistema de IA como as decisões humanas com eles relacionadas (p. ex., os domínios de aplicação de um sistema de IA). A explicabilidade técnica exige que as decisões tomadas por um sistema de IA possam ser compreendidas e rastreadas por seres humanos. Além disso, poderá ser necessário adotar soluções de compromissos entre o reforço da explicabilidade de um sistema (o que poderá reduzir a sua exatidão) ou o aumento da sua exatidão (à custa da sua explicabilidade). Sempre que um sistema de IA tenha um impacto significativo na vida das pessoas, deverá ser possível solicitar uma explicação adequada do respetivo processo de tomada de decisões. Tal explicação deve ser oportuna e adaptada ao nível de especialização da parte interessada em causa (p. ex., leigo, regulador ou investigador). Além disso, devem ser disponibilizadas explicações sobre o grau de influência e de intervenção de um sistema de IA no processo decisório da organização, as opções de conceção do sistema e os fundamentos da sua implantação (assegurando assim a transparência do modelo de negócio). *Prevenção de enviesamentos injustos*. Os conjuntos de dados utilizados pelos sistemas de IA (tanto para treino como para funcionamento) podem ser afetados pela inclusão de desvios históricos inadvertidos, bem como por lacunas e por maus modelos de governação. A manutenção de tais desvios pode dar origem a discriminação e preconceitos (in)diretos não intencionais contra determinados grupos ou pessoas, agravando o preconceito e a marginalização. A exploração intencional de preconceitos já existentes (entre os consumidores) e as práticas de concorrência desleal, tais como a homogeneização dos preços através de conluios ou da falta de transparência do mercado, também podem causar danos. O enviesamento identificável e discriminatório deve ser eliminado na fase de recolha de dados, sempre que possível. A forma como os sistemas de IA são desenvolvidos (p. ex., a programação de algoritmos) também pode ser afetada por um enviesamento injusto. Tal pode ser combatido mediante a adoção de processos de supervisão para analisar e abordar a finalidade, os condicionalismos, os requisitos e as decisões do sistema de forma clara e transparente. Além disso, o recrutamento de pessoal de diferentes origens, culturas e disciplinas pode

Exemplificando este importante debate, a empresa Amazon criou um sistema de inteligência artificial, no ano de 2018, para auxiliar no recrutamento de candidatos. Este sistema (*software*) não conseguia selecionar candidatas mulheres. O sistema recrutava apenas candidatos homens para concorrer à vaga de emprego. Os especialistas da área de tecnologia empreenderam esforços no sentido de corrigir esse viés discriminatório constante no sistema, entretanto, não conseguiram resolver o problema. A empresa Amazon abandonou o projeto, consequentemente.[137]

O exemplo do sistema informático que pode conter viés discriminatório (discriminação algorítmica) deveria servir de oportunidade para criação de *softwares* que se coadunem com os direitos e garantias fundamentais. Segundo Harari[138], é mais fácil corrigir um sistema informático do que livrar os humanos de seus vieses racistas. Entretanto, sempre haverá o perigo do autor de um *software*, de algum modo, incluir seus vieses subconscientes no sistema.

Por isso, a realização de constantes testes nos sistemas informáticos são fundamentais para a necessária obediência aos direitos fundamentais dos titulares dos dados pessoais, desde a concepção do *software* e por padrão, destacando a importância da utilização das técnicas de *privacy by design* e *privacy by default*, preocupadas com o desenho e o acompanhamento da tecnologia em conformidade com a proteção dos direitos fundamentais de seus usuários.

No âmbito no trabalho realizado em plataformas digitais é preciso que se ressaltem aspectos fundamentais sobre a compreensão do tema. É verdade que o art. 20 da LGPD dispõe sobre o direito do titular de dados pessoais solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

A opção do legislador brasileiro foi diversa da opção do legislador europeu. Como predito, a LGPD foi alterada pela lei nº 13.853/2019. Antes dessa alteração legislativa, a LGPD previa no *caput* do artigo 20 que o titular dos dados teria o direito a solicitar revisão, por pessoa natural, das decisões tomadas com base em

---

assegurar a diversidade de opiniões e deve ser incentivado. (HIGH-LEVEL EXPERT GROUP ON AI (AI HLEG). **Ethics Guidelines for Trustworthy AI.** Bruxelas: European Commission, 2019. Disponível em: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>. Acesso em: junho de 2019).

[137] SALOMÃO, Karen. **Robô criado pela Amazon para buscar candidatos discriminava mulheres.** Revista Exame, São Paulo, 12 de outubro de 2018. Disponível em: <https://exame.abril.com.br/negocios/robo-criado-pela-amazon-para-buscar-candidatos-discriminava-mulheres/>. Acesso em: novembro de 2019.

[138] HARARI, Yuval Noah. **21 Lições para o Século 21**. 1. ed. São Paulo: Companhia das Letras, 2018, p. 87-88.

tratamento automatizado. Entretanto, a alteração legislativa retirou a expressão "por pessoa natural", ou seja, no Brasil, as decisões tomadas com base em tratamento automatizado poderão ser revistas, também, de forma automatizada, e não necessariamente por pessoa natural. Repise-se: por opção do legislador brasileiro!

Embora seja louvável reconhecer que no âmbito internacional, para além das previsões contidas no RGPD, a recente Diretiva (EU) 2024/2831 do Parlamento Europeu e do Conselho, de 23 de outubro de 2024, passou a dispor sobre as melhorias das condições de trabalho em plataformas digitais e também previu em seu art. 11 quanto às especificidades e necessidade de revisão humana.[139]

[139] "*Artigo 11.º* Revisão humana. 1. Os Estados-Membros asseguram que as pessoas que trabalham em plataformas digitais têm o direito a obter, sem demora injustificada, uma explicação verbal ou por escrito da plataforma de trabalho digital sobre qualquer decisão tomada ou apoiada por um sistema automatizado de tomada de decisões. A explicação é apresentada de forma transparente e inteligível, utilizando uma linguagem clara e simples. Os Estados-Membros asseguram que as plataformas de trabalho digitais preveem o acesso das pessoas que nelas trabalham a uma pessoa de contacto, designada pela plataforma, para analisar e clarificar os factos, as circunstâncias e os motivos que levaram à decisão. As plataformas de trabalho digitais asseguram que essas pessoas de contacto dispõem da competência, formação e autoridade necessárias para exercer essa função.
As plataformas de trabalho digitais facultam às pessoas que trabalham em plataformas digitais uma declaração escrita dos motivos de qualquer decisão tomada ou apoiada por um sistema automatizado de tomada de decisões que restrinja, suspenda ou encerre a conta da pessoa que trabalha em plataformas digitais, de qualquer decisão de recusa do pagamento pelo trabalho efetuado pela pessoa que trabalha em plataformas digitais, de qualquer decisão que afete a situação contratual da pessoa que trabalha em plataformas digitais, de qualquer decisão com efeitos semelhantes ou de qualquer outra decisão que afete os aspetos essenciais do trabalho ou de outras relações contratuais, sem demora injustificada, e, o mais tardar, na data em que essa decisão produzir efeitos.
2. As pessoas que trabalham em plataformas digitais e, em conformidade com o direito ou práticas nacionais, os representantes das pessoas que trabalham em plataformas digitais que atuam em nome das mesmas têm direito a solicitar à plataforma de trabalho digital que reveja as decisões a que se refere o n.º 1. A plataforma de trabalho digital responde a esse pedido dando à pessoa que trabalha em plataformas digitais uma resposta suficientemente precisa e devidamente fundamentada, sob a forma de documento escrito, que pode ser em formato eletrónico, sem demora injustificada e, em qualquer caso, no prazo de duas semanas a partir da data de receção do pedido.
3. Caso a decisão a que se refere o n.º 1 viole os direitos de uma pessoa que trabalha em plataformas digitais, a plataforma de trabalho digital retifica-a sem demora e, em qualquer caso, no prazo de duas semanas a contar da adoção da decisão. Se tal retificação não for possível, a plataforma de trabalho digital oferece uma compensação adequada pelos danos sofridos. Em qualquer caso, a plataforma de trabalho digital toma as medidas necessárias, incluindo, se adequado, a alteração do sistema automatizado de tomada de decisões ou a interrupção da sua utilização, a fim de evitar tais decisões no futuro.
4. O presente artigo não afeta os procedimentos disciplinares e de despedimento previstos no direito, convenções coletivas e práticas nacionais.

Entretanto, o art. 8 da CLT[140] deixa claro que a legislação estrangeira somente poderia ser utilizada na falta de disposições legais ou contratuais. Não é o caso ora em comento, pois o sistema brasileiro de proteção de dados pessoais prevê o direito à revisão de tomada de decisões automatizadas, nos moldes do que preconiza o art. 20 da LGPD. Ao ordenamento jurídico brasileiro, não haveria que se falar, neste passo, em aplicação ou na utilização da Diretiva (EU) 2024/2831 para que as revisões das decisões automatizadas sejam, necessariamente, revistas por pessoas naturais (revisão humana contida no art. 11 da Diretiva (EU) 2024/2831).

Neste ínterim, eventuais decisões tomadas de forma automatizada poderão ser revistas também de forma automatizada, nos termos da atual leitura do art. 20 da LGPD.

Contudo, importa frisar o risco de reprodução de vieses existentes, uma vez que sistemas automatizados treinados com dados enviesados tendem a perpetuar preconceitos e discriminações presentes nos dados de origem. Uma revisão automatizada pode não identificar ou corrigir esses vieses, resultando em decisões igualmente falhas. Isso porque a revisão automatizada não possui a capacidade de avaliar aspectos subjetivos ou contextuais, potencializando injustiças. Embora a LGPD, não especifique que a revisão deva ser realizada por pessoa natural, a intervenção humana é essencial para assegurar que decisões automatizadas sejam justas, transparentes e livre de vieses.

2.1. Boa Prática: Revisão das decisões automatizadas por pessoa natural em Plataforma Digital

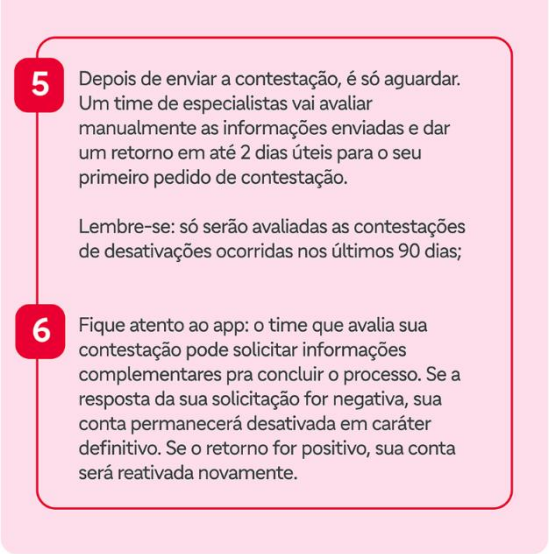
A título exemplificativo, a reconhecida Plataforma Digital de entregas "Ifood" possui diversos documentos publicados em seu sítio da internet, que contemplam os direitos fundamentais à proteção de dados pessoais, tanto de clientes (consumidores) quanto de entregadores (parceiros comerciais).

A Plataforma Ifood dispõe (e explica) as possibilidades de restrição, parada técnica, bloqueio e desativação da plataforma. Em atendimento ao art. 20 da LGPD (revisão de decisão tomada de forma

5. O presente artigo não se aplica às pessoas que trabalham em plataformas digitais que sejam também utilizadores profissionais na aceção do artigo 2.º, ponto 1, do Regulamento (UE) 2019/1150." (Disponível em: <Diretiva- UE-2024/2831- EN- EUR-Lex >)

[140] "Art. 8º- As autoridades administrativas e a Justiça do Trabalho, na falta de disposições legais ou contratuais, decidirão, conforme o caso, pela jurisprudência, por analogia, por eqüidade e outros princípios e normas gerais de direito, principalmente do direito do trabalho, e, ainda, de acordo com os usos e costumes, o direito comparado, mas sempre de maneira que nenhum interesse de classe ou particular prevaleça sobre o interesse público. § 1º O direito comum será fonte subsidiária do direito do trabalho." (BRASIL. **Lei 13.467, de 13 de julho de 2017**. Dispõe sobre a alteração da Consolidação das Leis do Trabalho. Brasília, 2017. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13467.htm>. Acesso em: dezembro de 2024).

automatizada), a Plataforma Ifood prevê o direito de contestação. O direito de contestação envolverá a revisão humana e a equipe de especialistas da referida Plataforma retornará com a resposta ao titular (direito à explicabilidade) em até dois dias. Sobre o direito de contestação de desativações da Plataforma, observe-se a clareza com que a Plataforma Ifood atende aos direitos dos titulares de dados pessoais[141]:



Não bastasse isso, importa registrar o Aviso de Privacidade exposto no site da Plataforma. Absolutamente ilustrativo, legível, informativo, atendendo muito bem à finalidade de comunicação ao titular de dados pessoais (entregadores parceiros). Veja-se[142]:

[141] Acesso em: < Entenda como contestar uma desativação - iFood Entregadores>
[142] Acesso em: < Declaração de Privacidade iFood para Entregadores - iFood Entregadores>

Além dos documentos destinados ao "Direito de Contestação" das decisões tomadas de forma automatizada, conforme acima exposto, bem como o documento intitulado "Declaração de Privacidade Ifood para Entregadores", a Plataforma Ifood ainda disponibiliza os seus "Termos e Condições de Uso Ifood para Entregadores", totalmente em conformidade com o que dispõe a LGPD, com um passo a passo que esmiuça a necessidade de fornecimento de dados pessoais para a execução do próprio contrato entabulado entre as partes, mais uma vez, de forma legível, ilustrativa e absolutamente compreensível pelo público de entregadores parceiros, e em atenção à base legal da execução do contrato. Observe-se[143]:

[143] Acesso em: "Termos-e-condicoes-v2022_Ajustado"

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

Conforme exposto anteriormente, pela leitura dos artigos do Regulamento Europeu e da Lei Geral de Proteção de Dados Brasileira, é possível concluir que o empresário poderá ser responsabilizado quando a utilização de um sistema de inteligência artificial prejudicar os direitos do titular dos dados pessoais (trabalhador). Entretanto, a depender das medidas adotadas pela empresa na utilização desse tipo de *software*, será possível isentar o empregador, ou a organização pública ou privada, de eventual responsabilidade.

A Lei Geral de Proteção de Dados, de acordo com o anteriormente exposto, em seu artigo 20, § 1º esclarece que o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil profissional, devendo o controlador (organização empresarial) fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada. O § 2º do artigo 20 prevê, inclusive, que no caso do não fornecimento das informações solicitadas, a autoridade nacional poderá realizar auditoria para verificar aspectos discriminatórios no tratamento automatizado de dados pessoais.

3. NEGOCIAÇÃO COLETIVA

O reconhecimento das convenções e acordos coletivos de trabalho, prevista no artigo 7º, XXVI da Constituição Federal, em conjunto com o papel dos sindicatos previsto no artigo 8º, III da CF/88, além das Convenções n. 98 e n. 154 da OIT, ratificadas pelo Brasil, destacam a importância desse instrumento negocial na relação entre empregadores e empregados e a necessidade de os países fomentarem e valorizarem as negociações coletivas como meio eficaz de estabelecer melhores condições de trabalho – com a intervenção coletiva em face do indivíduo, visando a proteção deste, dentro de uma relação naturalmente desigual e com discrepância de forças.

A negociação coletiva é forma autocompositiva de solução de conflitos, na qual os próprios interessados solucionam o embate, sem a interferência de terceiros. Com o sucesso da negociação coletiva, decorrem os seus instrumentos: a convenção coletiva de trabalho e o acordo coletivo de trabalho.[144]

Como forma de pacificação de conflitos coletivos trabalhistas, a negociação coletiva pressupõe igualdade entre dois sujeitos coletivos: de um lado, o sindicato dos trabalhadores, e de outro, o sindicato dos empregadores, ou a empresa. A coletivização dos trabalhadores proporciona paridade de armas e equilíbrio de forças e, da negociação coletiva, defluem os instrumentos normativos (acordos e convenções coletivas).[145]

---

[144] STÜRMER, Gilberto. **A Liberdade Sindical na Constituição da República Federativa do Brasil de 1988 e sua relação com a Convenção 87 da Organização Internacional do Trabalho.** Porto Alegre: Livraria do Advogado, 2007, p. 95.

[145] SANTOS, Enoque Ribeiro dos. **Negociação Coletiva de Trabalho**. 3. ed. rev. atual. Rio de Janeiro: Forense, 2018, p. 111-112.

E é nesse sentido que se pode dizer que a negociação coletiva trabalhista transcende o próprio Direito do Trabalho, pois, historicamente, desde o século XIX a atuação dinâmica e diversificada da negociação coletiva nas relações laborais sempre influenciou, de forma positiva, a estruturação democrática do conjunto social.[146]

Celebrada entre empregadores e trabalhadores (ou seus respectivos substitutos[147]), a negociação coletiva de trabalho é processo democrático de autocomposição de interesses pelos próprios atores sociais, com o objetivo de fixar condições de trabalho que se apliquem à coletividade de empregados de determinada empresa ou de uma categoria econômica.[148]

Um dos papeis da negociação coletiva, portanto, é assegurar direitos trabalhistas e individuais para os trabalhadores inseridos naquele contexto social e que, individualmente, e dentro do rol de direitos fundamentais garantidos pela Constituição Federal, soma-se o disposto no artigo 5º, LXXIX, incluído pela Emenda Constitucional n. 115/22, que trata sobre o direito à proteção de dados pessoais.

Recentemente, muito tem se falado sobre o trabalho plataformizado, assumido por empresas digitais na forma de aplicativos que "intermediam" o trabalho, na forma de "prestação de serviço", onde há precarização dos direitos trabalhistas e estímulo à uma suposta independência e autodeterminação do indivíduo como empregador de si mesmo, mas com vários instrumentos de coleta de dados e informações que visam controlar o trabalho exercido, inclusive por meio de algoritmos e decisões automatizadas.

A Constituição Federal dispõe de importantes artigos relacionados ao Direito Coletivo do Trabalho. Dentre os quais, o artigo 11 prevê que nas empresas de mais de 200 empregados é assegurada a eleição de um

---

[146] DELGADO, Maurício Godinho. **Curso de direito do trabalho**. 16. ed. rev. ampl. São Paulo: Editora LTr, 2017, p. 1559.

[147] Sobre a diferença entre representante e substituto processual, Chiovenda afirma: "As posições fundamentais e secundárias acima examinadas assume-as normalmente a própria pessoa que se afirma titular da relação deduzida em juízo. Mas excepcionalmente assume-as pessoa que não se afirma e apresenta como sujeito da relação substancial em litígio. Como no direito substancial casos se verificam em que se admite alguém a exercer no próprio nome direitos alheios, assim também outro pode ingressar em juízo no próprio nome (isto é, como parte) por um direito alheio. Ao introduzir e analisar essa categoria, porfiei em definir-lhe o caráter, atribuindo-lhe a denominação de substituição processual. Categoria e denominação hoje aceitas por todos. Muitos dos casos por mim incluídos em tal categoria são comumente explicados como casos de representação; mas, conquanto se produzam, aí, alguns efeitos análogos aos da representação, não é de representação que se trata, de vez que o representante processual age em nome de outro, de sorte que parte na causa é, na verdade, o representado; ao passo que o substituto processual age em nome próprio e é parte na causa. (CHIOVENDA, Giuseppe. **Instituições de direito processual civil**. Tradução de Paolo Capitanio. 2. ed. Campinas: Bookseller, 2000, p. 300-301).

[148] TEIXEIRA FILHO, João de Lima *et al*. **Instituições de direito do trabalho**. 16. ed., v. 2., São Paulo: Editora LTr, 1996, p. 1131.

representante destes, para promover o entendimento direto com os empregadores. Com a edição da Lei 13.467/2017 (reforma trabalhista), foi regulamentada a representação dos empregados nos artigos 510-A a 510-D.

A reforma trabalhista previu a criação de mais uma espécie de garantia de emprego: desde o registro da candidatura até um ano após o fim do mandato, o membro da comissão de representantes dos empregados não poderá sofrer despedida arbitrária, entendendo-se como tal aquela que não se fundar em motivo disciplinar, técnico, econômico ou financeiro.[149]

É importante mencionar, também, que a Lei 13.467/2017, ao regulamentar o artigo 11 da Constituição Federal, não assegura a eleição de apenas um representante dos empregados, mas uma comissão de representantes, cuja composição é definida pela quantidade de empregados na empresa, de acordo com o artigo 510-A da CLT.[150] Há dúvidas quanto à adesão prática e quanto ao apoio das entidades sindicais nesse tipo de representação dos empregados. Como essa espécie de representação poderia ser criada por norma coletiva, compreende-se ser desnecessária a sua criação por lei.[151]

Não obstante, o sistema de negociação começa dentro da empresa. O representante dos empregados além de tratar de salários, cuida, também, dos conflitos do dia a dia.[152] Esse mecanismo pode ser utilizado como

---

[149] "Art. 510-D. O mandato dos membros da comissão de representantes dos empregados será de um ano. § 3o Desde o registro da candidatura até um ano após o fim do mandato, o membro da comissão de representantes dos empregados não poderá sofrer despedida arbitrária, entendendo-se como tal a que não se fundar em motivo disciplinar, técnico, econômico ou financeiro." (BRASIL. **Lei 13.467, de 13 de julho de 2017**. Dispõe sobre a alteração da Consolidação das Leis do Trabalho. Brasília, 2017. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13467.htm>. Acesso em: março de 2019).

[150] "Art. 510-A. Nas empresas com mais de duzentos empregados, é assegurada a eleição de uma comissão para representá-los, com a finalidade de promover-lhes o entendimento direto com os empregadores. § 1o A comissão será composta: I- nas empresas com mais de duzentos e até três mil empregados, por três membros; II- nas empresas com mais de três mil e até cinco mil empregados, por cinco membros; III- nas empresas com mais de cinco mil empregados, por sete membros." (BRASIL. **Lei 13.467, de 13 de julho de 2017**. Dispõe sobre a alteração da Consolidação das Leis do Trabalho. Brasília, 2017. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13467.htm>. Acesso em: março de 2019).

[151] FINCATO, Denise; STÜRMER, Gilberto. **A reforma trabalhista simplificada:** comentários à Lei nº 13.467/2017. Porto Alegre: EDIPUCRS, 2019, p. 61-62.

[152] STÜRMER, Gilberto. Negociação Coletiva de Trabalho como Direito Fundamental. **Revista Justiça do Direito**, v. 31, n. 2, mai./ago. 2017, p. 409-431, p. 425.

filtro para reduzir as demandas judiciais e oportuniza auxiliar na conformação da tecnologia no ambiente laboral, permitindo melhor entendimento entre empregados e empregador.

Este canal de comunicação direto dos empregados com o empregador no ambiente de trabalho é extremamente relevante. Entretanto, insta referir que eventual acordo celebrado pela comissão de representação dos empregados não terá a mesma força normativa que a celebração de um acordo ou de uma convenção coletiva de trabalho, não servindo a comissão de representantes dos empregados para substituir o sindicato em juízo, ou fora dele. O artigo 8º, incisos III e VI da Constituição Federal deixa claro que somente os sindicatos são partes legítimas para a negociação coletiva.[153] A regulamentação do artigo 11 da Constituição Federal, com a inserção dos artigos 510-A a 510-D da CLT, tem a finalidade de buscar entendimento e diálogo social, mas não solapar a autoridade dos sindicatos.[154]

A Constituição Federal reconhece a autonomia privada coletiva, as convenções e os acordos coletivos de trabalho em seu artigo 7º, incisos VI, XIII e XXVI, e a negociação coletiva no artigo 7º, inciso XIV e no artigo 8º inciso VI, incluindo o tema no rol dos direitos fundamentais sociais. A negociação coletiva, enquanto direito fundamental social, possui uma dimensão negativa (direito de defesa) e uma dimensão positiva, ou prestacional, e a sua proteção constitui exigência e concretização da dignidade da pessoa humana[155] sendo considerada como a "essência" do Direito do Trabalho. De acordo com Silva[156]:

> Não fosse pelo poder de negociação coletiva, talvez o direito do trabalho ainda estivesse inserido em algum apêndice do direito civil, pois não passaria de um acervo sobre relação jurídica que une trabalhador, empreendimento de sua energia e empregador. Porém, esse empenho da energia humana é feito mediante algumas peculiaridades muito caras ao direito do trabalho. [...] A negociação coletiva tem

[153] "Art. 8º É livre a associação profissional ou sindical, observado o seguinte: III - ao sindicato cabe a defesa dos direitos e interesses coletivos ou individuais da categoria, inclusive em questões judiciais ou administrativas; VI - é obrigatória a participação dos sindicatos nas negociações coletivas de trabalho". (BRASIL. **Constituição da República Federativa do Brasil**, de 05 de outubro de 1988. Brasília, DF: Senado Federal, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: novembro de 2019).

[154] SILVA, Homero Batista Mateus da. **Comentários à Reforma Trabalhista:** análise da lei 13.467/2017 - artigo por artigo. 2 ed. rev. atual. São Paulo: Editora Revista dos Tribunais, 2017, p. 124-125.

[155] SARLET, Ingo Wolfgang. **Dignidade da Pessoa Humana e Direitos Fundamentais**. Porto Alegre: Livraria do Advogado, 2001, p. 92.

[156] SILVA, Homero Batista Mateus da. **Curso de direito do trabalho aplicado.** Vol. 7 – Direito Coletivo do Trabalho. 3. ed. rev. atual. ampl. São Paulo: Editora Revista dos Tribunais, 2015, p. 157.

> diversos níveis, desde aqueles restritos ao âmbito das empresas até aqueles de âmbito nacional, comunitário ou global, passando pela forma mais corriqueira do acerto entre duas entidades sindicais de campos opostos.

No que tange à negociação coletiva, a reforma trabalhista passou a dispor no artigo 611-A as hipóteses em que a convenção coletiva e o acordo coletivo de trabalho terão prevalência sobre a lei, e no artigo 611-B as matérias que não poderão ser reduzidas ou suprimidas por negociação coletiva de trabalho, por serem direitos fundamentais sociais, inscritos na Constituição Federal.[157]

O artigo 611-B da CLT prevê os direitos que não poderão ser suprimidos, ou reduzidos, não significando dizer que não possa haver negociação sobre eles. É possível negociar o modo de gozo do direito. Assim, como exemplo, não se pode reduzir ou suprimir o 13º salário, de acordo com o artigo 611-B, inciso V. Entretanto, há a possibilidade de negociar a forma de seu pagamento, fazendo-o antecipadamente ou de forma fracionada mensal.[158] E isto se coaduna com a previsão do artigo 7º da Constituição Federal, na medida em que o artigo 611-B da CLT reflete o rol de cláusulas pétreas inscritos no artigo 7º da Lei Maior.[159]

O artigo 611-B da CLT deverá funcionar como cláusula de barreira, para que se possa conferir liberdade na negociação, observando os direitos fundamentais dos trabalhadores, tendo em vista a supremacia da negociação coletiva em relação ao previsto na legislação. Neste sentido, teremos um Direito do Trabalho menos rígido e formal, com maior neutralidade e maleabilidade, desprovido de seu núcleo protetor e de sua tríplice vertente (norma mais favorável, condição mais benéfica e *in dubio pro operario*).[160]

Pode-se dizer que a inserção de diversos temas envolvendo a proteção de dados pessoais, no âmbito das negociações coletivas, traria maior segurança tanto à categoria econômica quanto à categoria profissional.

Neste aspecto, poder-se-ia pensar que o artigo 611-B, inciso XVII vedaria a inserção do tema em acordo ou convenção coletiva de trabalho, sob a justificativa de se referir a normas de saúde, higiene e segurança do

---

[157] BRASIL. **Decreto-lei 5.452, de 01º de maio de 1943.** Aprova a Consolidação das Leis do Trabalho. Brasília, 1943. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/Del5452.htm>. Acesso em: janeiro de 2020.

[158] MARQUES DE LIMA, Francisco Meton; MARQUES DE LIMA, Francisco Péricles Rodrigues. **Reforma Trabalhista.** Entenda ponto por ponto.São Paulo: Editora LTr, 2017, p. 104.

[159] FINCATO, Denise; STÜRMER, Gilberto. **A reforma trabalhista simplificada:** comentários à Lei nº 13.467/2017. Porto Alegre: EDIPUCRS, 2019, p. 71.

[160] SANTOS, Enoque Ribeiro dos. **Negociação Coletiva de Trabalho**. 3. ed. rev. atual. Rio de Janeiro: Forense, 2018, p. 333.

trabalho. Entretanto, desde já, deve-se deixar claro que o objetivo da inserção em negociação coletiva de temas envolvendo a proteção de dados pessoais dos empregados não é o de reduzir ou suprimir direitos.

Ao contrário, o intuito é adequar a relação de emprego ao uso da tecnologia avançada no ambiente laboral, servindo a negociação coletiva e a possibilidade de inserção do tema em acordo coletivo de trabalho ou convenção coletiva de trabalho como forma de conferir maior segurança jurídica ao empregador e, também, ao empregado, em consonância com os direitos fundamentais.

Portanto, muito há que se falar e proteger no âmbito da proteção de dados junto à negociação coletiva, que deve assumir papel cada vez mais relevante em face da crescente automação e avanço da tecnologia nas relações de trabalho, com papel relevante a ser desempenhado por Sindicatos, associações e cooperativas junto à ANPD, visando a proteção dos dados funcionais e os direitos dos trabalhadores.

Por coincidência ou não, o artigo da constituição que reconhece a negociação coletiva é sucedido pelo inciso XXVII do referido artigo, que trata sobre a proteção do trabalhador em face da automação, a ser regulamentado por lei, o que até hoje, ultrapassados 36 anos do texto constitucional, não aconteceu pelo Congresso Nacional, destacando ainda mais o papel central que terão Sindicatos e ANPD na proteção do trabalhador face o uso da inteligência artificial.

Por todo o exposto, demonstra-se o papel central das negociações coletivas e do incentivo destas no cenário nacional, centrada na defesa dos interesses e dos direitos dos trabalhadores, hipossuficientes nas relações empregatícias, e que são mais sucessíveis a descasos e violações à LGPD, com papel sindical de apoio à fiscalização e cumprimento da proteção de dados no território nacional.

3.1 Boas Práticas Globais para Proteção de Dados na Negociação Coletiva

1. Cláusulas Específicas em Acordos Coletivos:
    a. Definir limites para monitoramento e coleta de dados.
    b. Garantir consentimento livre, informado e inequívoco para finalidades determinadas, para usos não essenciais.
    c. Garantir Revisão Humana em decisões automatizadas
2. Participação Sindical em Decisões Tecnológicas:
    a. Envolver sindicatos na implantação de tecnologias que utilizem dados dos trabalhadores.

3. Transparência e Prestação de Contas:
    a. Comunicação clara sobre como e por que os dados são tratados.
4. Educação e Treinamento:
    a. Sensibilizar trabalhadores e empregadores sobre direitos de proteção de dados.

Por que regulamentar via Negociação Coletiva?

- Flexibilidade:
    - Regras adaptadas à realidade do setor ou da empresa.
- Fortalecimento da Proteção:
    - Complementa legislações nacionais e cria garantias adicionais.
- Prevenção de Conflitos:
    - Acordos claros evitam litígios relacionados à privacidade e ao uso indevido de dados.

V- Desafios e Pontos de Melhoria

O tratamento de dados de trabalhadores está no centro do debate global sobre privacidade e dignidade no trabalho. A experiência de países como França, Alemanha e Reino Unido, que aliam proteção de dados à negociação coletiva, pode servir de exemplo para o Brasil. Uma política nacional de proteção de dados no trabalho deve incorporar princípios como:

1. Dados de Qualidade e Vieses Discriminatórios

A gestão algorítmica, quando alimentada por dados de baixa qualidade ou enviesados, pode perpetuar discriminações e desigualdades.

• Proposta: Desenvolver diretrizes obrigatórias para auditoria e validação de algoritmos, garantindo que sejam justos e não discriminatórios.

2. Transparência na Gestão Algorítmica

Os trabalhadores muitas vezes desconhecem como seus dados são utilizados ou os critérios de decisões automatizadas.

• Proposta: Garantir a explicabilidade sobre o funcionamento dos algoritmos e disponibilizar canais para contestação de decisões.

3. Limitações do Consentimento

O consentimento, enquanto base legal, é limitado no contexto laboral devido à assimetria de poder entre empregador e empregado.

• Proposta: Priorizar bases legais mais robustas, como a execução de contrato ou cumprimento de obrigação legal, evitando que o consentimento seja utilizado de forma coercitiva.

4. Negociação Coletiva e Representação dos Trabalhadores

A negociação coletiva pode equilibrar a relação de poder e estabelecer salvaguardas claras para o tratamento de dados no trabalho.

• Proposta: Incentivar as negociações coletivas sobre o uso de dados no ambiente de trabalho.

Normas internacionais como o GDPR e legislações nacionais como a LGPD desempenham um papel crucial na proteção de dados no contexto laboral, mas ainda há lacunas a serem preenchidas. Dados de qualidade, transparência e negociação coletiva são pilares fundamentais para enfrentar os desafios impostos pela digitalização do trabalho, como vieses algorítmicos e limitações do consentimento. A construção de uma política nacional integrada, alinhada às melhores práticas globais, é essencial para proteger os direitos dos trabalhadores e fomentar relações laborais mais justas e equilibradas.

VI- Conclusão

O discurso jurídico atual é permeado pela ideia do risco. A velocidade da inovação e das constantes descobertas tecnológicas não vem acompanhada pela análise de seus efeitos. Esse descompasso traz a importância da gestão dos riscos laborais no âmbito do direito à proteção de dados pessoais, pois o conhecimento sobre suas consequências importa na necessidade de maior segurança jurídica nas relações negociais. Mais do que isso: volta o olhar para a importância da ética negocial, não como uma questão moral, mas sim, legal.

Dessa forma, Beck afirma que a diferença de todas as épocas anteriores (incluída a sociedade industrial) para a sociedade de risco é que essa sociedade se caracteriza essencialmente por uma carência: a impossibilidade de prever externamente as situações de perigo. A diferença de todas as culturas anteriores e todas as fases sociais que se enfrentaram de diversos modos com ameaças é que a atual sociedade se encontra confrontada consigo mesma em relação aos riscos.[161]

A descoberta de novas tecnologias e a intensidade do progresso da ciência não foi seguida de instrumentos de avaliação e medição dos potenciais resultados de sua aplicação. Conforme Bottini:[162]

> Do descompasso entre o surgimento de inovações científicas e o conhecimento das consequências de seu uso surge a incerteza, a insegurança, que obrigam o ser humano a lidar com o risco sob uma nova perspectiva. O risco, fator indispensável ao desenvolvimento econômico de livre mercado, passa a ocupar papel central no modelo de organização social. O risco torna-se figura crucial para a organização coletiva, passa a compor o núcleo da atividade social, passa a ser sua essência. Surge a sociedade de riscos.

A verdade é que não podemos parar de questionar. A postura proativa, *ex ante*, de antecipação a riscos num cenário *Big Data* remete à imposição de assunção de responsabilidade da sociedade em que vivemos.

Nessa esteira, Bauman refere que são os padrões éticos, muito mais do que a racionalidade e a diligência, que estão em crise. Devemos tomar a decisão de assumir a responsabilidade por nossa responsabilidade, a decisão de medir a qualidade da sociedade pela qualidade de seus padrões éticos.[163] De acordo com o sociólogo francês Morin: "o mundo sempre comportará riscos, imprevistos, incertezas, mas também poderá comportar capacidades criadoras, desenvolvimento da compreensão e da bondade, nova consciência humana."[164]

Na visão de Beck, o mundo não está apenas mudando. Está em constante metamorfose. O autor designa o termo "risco digital global" para afirmar que a valoração desse risco difere dos demais (risco

---

[161] BECK, Ulrich. **La sociedad del riesgo hacia una nueva modernidad**. Barcelona: Paidós, 1998, p. 237.

[162] BOTTINI, Pierpaolo Cruz. Princípio da precaução, direito penal e sociedade de risco. **Revista Brasileira de Ciências Criminais,** São Paulo, n. 61, p. 44-121, jul./ago. 2006, p. 48.

[163] BAUMAN, Zygmunt. **A sociedade individualizada:** vidas contadas e histórias vividas. Rio de Janeiro: Zahar, 2008, p. 109.

[164] MORIN, Edgar. **Rumo ao Abismo?** Ensaio sobre o destino da humanidade. Rio de Janeiro: Bertrand Brasil, 2011, p. 190.

financeiro, risco climático, risco ao terrorismo), pois o risco digital global afeta a liberdade digital. Trata-se de uma ameaça imaterial. Não é uma ameaça para a vida (terrorismo), para a sobrevivência da humanidade (risco climático), ou para a propriedade privada (risco financeiro). A violação da liberdade digital não é dolorosa. Não se padece de uma enfermidade, nem se arrasta a uma inundação, nem nos falta oportunidade para encontrar trabalho. A liberdade morre sem que os seres humanos saiam feridos fisicamente. O risco da falta de liberdade digital supõe uma ameaça para algumas das maiores conquistas da civilização moderna: a liberdade pessoal, a autonomia, a intimidade, que são instituições básicas da democracia e do Direito, nas quais também se fundamentam o Estado.[165]

Em interessante estudo elaborado por Gasser e Haeusermann, sobre a importância do *compliance* e da gestão de riscos provenientes do avanço da tecnologia, os autores afirmam que, de forma reativa à rede digital e à informatização, a necessária gestão de riscos na interrelação do Direito com a tecnologia da informação e o mercado faz surgir uma forma mais ampla de *compliance*, que convencionam chamar de "*e-compliance*". Os autores defendem uma abordagem integrada e abrangente do conceito de conformidade, que leve em consideração o ritmo da digitalização, favorecendo o ajuste do sistema jurídico às mudanças tecnológicas que afetam as empresas e que impõem constantes alterações nas organizações corporativas. Este grande desafio multidisciplinar, que exige a interconexão entre Direito e tecnologia da informação, representa o que convencionam os autores em designar de "*e-compliance*".[166]

O gerenciamento de riscos provenientes das inovações tecnológicas, em que a dinâmica digital das relações dificilmente encontra respaldo jurídico adequado, requer um diálogo do Direito com a tecnologia avançada, que seja pautado na observância dos princípios da prevenção de danos e da precaução de riscos, na tentativa de construção de um cenário que minimize riscos e potencialize o desenvolvimento econômico digital, com a devida proteção dos direitos fundamentais.

Portanto, a necessidade de adequar o avanço da tecnologia e a exploração massiva de dados pessoais no ambiente de trabalho reforça a importância da implementação de um sistema de *compliance* trabalhista digital, com ênfase no interesse e na preservação dos direitos fundamentais do empregado e do empregador, num contexto produtor de incessantes riscos e oportunidades de desenvolvimento.

---

[165] BECK, Ulrich. **La metamorfosis del mundo**. 1. ed. Barcelona: Paidós, 2017, p. 165.

[166] GASSER, Urs; HAEUSERMANN, Daniel M. E-compliance: towards a roadmap for effective risk management. **The Berkman Center for Internet & Society**. Cambridge, n. 2007-3, mar. 2007, p. 10-11. Disponível em: <https://www.semanticscholar.org/paper/E-Compliance%3A-Towards-a-Roadmap-for-Effective-Risk-Gasser-H%C3%A4usermann/ddb0222b96a0d76468ced83deaadd27661d504dc>. Acesso em: novembro de 2019.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

A conformidade com a Lei Geral de Proteção de Dados (LGPD) no contexto das relações de trabalho, especialmente em processos de recrutamento e seleção, exige uma abordagem estruturada e transparente, baseada nos princípios fundamentais da legislação. A eliminação de práticas inadequadas, como o uso de consentimento forçado e genérico, é fundamental para garantir que as finalidades do tratamento sejam claramente definidas, específicas e vinculadas às bases legais apropriadas.

Respeitar os direitos dos titulares, incluindo a liberdade de recusar consentimento em finalidades acessórias e a possibilidade posterior de revogação, reflete não apenas uma obrigação legal, mas também um compromisso ético das empresas. Além disso, a adoção de práticas como o consentimento granular e o fornecimento de informações detalhadas em avisos de privacidade fortalece a confiança dos candidatos nos processos seletivos.

Ressalte-se que o tratamento de dados de titulares empregados, após a contratação, também exige o cumprimento rigoroso dos princípios de transparência e fornecimento de informações claras. As empresas devem garantir que todos os funcionários compreendam como e por que seus dados são tratados, restringir o tratamento de dados ao estritamente necessário e incentivar a negociação coletiva para estabelecer limites e salvaguardas no uso de tecnologias, promovendo um ambiente de trabalho ético e respeitoso.

Essa postura proativa não apenas assegura a proteção dos dados pessoais, mas também contribui para a construção de um ambiente de trabalho mais justo, equitativo e alinhado aos valores de privacidade e transparência. Empresas que demonstram esse compromisso fortalecem a confiança dos candidatos e funcionários, consolidando sua reputação em um mercado cada vez mais atento às questões de privacidade e proteção de dados.

Adotar essas práticas vai além da conformidade com a LGPD: é um passo essencial para promover uma cultura de respeito à privacidade e ética nas relações de trabalho.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANEXO XXII – ESTUDO DE CASO: EMPREENDEDORISMO E EMPREENDEDORISMO SOCIAL

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

Estudo de Caso

Empreendedorismo e empreendedorismo social

Conselheiro: Alexandre Boava

dezembro/2024

Esse estudo de caso tem como objetivo abordar o inciso "V" do Artigo 2º da LGPD, a partir de um de seus fundamentos, o desenvolvimento econômico, tecnológico e inovação aplicado ao empreendedorismo e ao empreendedorismo social. Para melhor compreensão do que se trata pensar em proteção de dados para o desenvolvimento é importante delimitar a quais atores esse estudo se propõe a dialogar.

Como empreendedores são considerados:

- trabalhadores autônomos;
- "MEIs";
- pequenos negócios;
- pequenas cooperativas.

E como empreendedores sociais:

- associações
- organizações filantrópicas
- pessoas jurídicas sem fins lucrativos.

Foi identificado 3 aspectos principais para trazer mais desenvolvimento e segurança jurídica para esses atores,

- primeiro abarca todas iniciativas e tem a ver com o que chamamos de aculturamento que passa por orientação, instrução, informação, formação e letramento para essas pessoas jurídicas e profissionais autônomos;
- segundo é disponibilizar tecnologias/ferramentas digitais livres e auditáveis que facilitem o trabalho de governança e segurança dos dados;
- terceiro diz respeito a capacidade de financiamento de seus negócios em que os dados desses atores devem seguir a Lei Geral de Proteção de Dados Pessoais.

1. Orientação e aculturamento

Grande parte da sociedade carece de sensibilização e maior compreensão de quais são os direitos garantidos pela LGPD, isso se reflete na atuação empreendedora de cada uma dessas pessoas. Levar a cultura de proteção de dados, os deveres e limites que a LGPD impõe é fundamental para que haja mais segurança jurídica para esses atores economicamente menores, e fortalece a garantia dos direitos dos titulares de dados.

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

Neste estudo destacamos os princípios da LGPD de finalidade e necessidade. Esses princípios garantem que os dados dos titulares de dados pessoais captados serão utilizados especificamente para uma certa aplicação, não devendo existir a captação de dados que não se aplicam à finalidade informada ao titular. A importância de solicitar, captar, armazenar e processar apenas dados que são de fato úteis para a organização traz mais segurança jurídica e segurança da informação, isso se deve pelo caráter não excessivo da captação de dados. Não é permitido pela LGPD que se capte e armazene dados que não serão utilizados, isso se dá para que não haja um acúmulo de dados que podem ser expostos de maneira a nem serem aproveitados o seu valor real, expondo titulares, aumentando os riscos de vazamento de dados e elevando os custos e a complexidade da manutenção.

Propomos o fortalecimento de ações que conscientizem a esses pequenos controladores de dados da importância de lidar com os dados pessoais com responsabilidade e como isso traz segurança jurídica para os seus negócios, uma vez que a exposição a um tratamento irregular do ponto de vista dos direitos do titular e o vazamento de dados em excesso, causa grandes prejuízos.

Segue exemplos brasileiros que devem ser fortalecidos e expandidos, dialogando com os estados e municípios, criando agendas de conscientiação em cada território, a fim de levar para mais próximo do controlador de dados uma compreensão mais adequada de como se proteger e proteger os dados de seus clientes e fornecedores (titulares de dados),

- ANPD: Glossário de Proteção de Dados Pessoais e Privacidade;
- ANPD: Guia Orientativo sobre segurança da informação para agentes de tratamento de pequeno porte;
- Parceria ANPD e Nic.br:
  - Fascículo: Vazamento de Dados
  - Fascículo: Proteção de Dados
- IDEC: Manual Prático de Adequação a Lei Geral de Proteção de Dados para Micro e Pequenas Empresas

Exemplos internacionais,

País	Iniciativa	Descrição	Impacto

Reino Unido	Guia para pequenas empresas e startups sobre proteção de dados	O ICO oferece guias, checklists e cursos online gratuitos para ajudar pequenas empresas a entenderem suas obrigações sob a GDPR.	Reduz riscos legais e melhora a conformidade de empresas menores.
Canadá	Ferramentas de orientação para empresas	Oferece guias específicos, vídeos e seminários sobre como gerenciar dados pessoais de maneira responsável sob a lei PIPEDA.	Melhora o entendimento das normas de privacidade e segurança de dados.
União Europeia	Kit de ferramentas para Empresas	Inclui um portal interativo com orientações personalizadas para ajudar empresas a implementarem medidas de proteção de dados.	Apoia o cumprimento das obrigações legais de forma acessível e prática.

Links

Reino Unido: https://ico.org.uk/for-organisations

Canadá: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/

União Europeia: https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en

2. Ferramentas e procedimentos de segurança

No cenário atual, as pequenas iniciativas utilizam ferramentas para o tráfego de dados que podem ou não ser adequadas para um tratamento correto dos dados. Via de regra a escolha do aparato tecnológico digital que suportar essas ações se dá pela facilidade de utilização e/ou aquisição, ou seja, ferramentas comuns de mercado que se utiliza na sociedade brasileira como um todo, como Whatsapp/Whatsapp Business, Google Drive, Gmail, Planilhas Google, Wordpress, Wix, entre muitas outras, que se caracterizam por serem

amplamente utilizadas e pelo custo acessível. Essas ferramentas apesar de cada uma ter suas políticas de dados e arquiteturas de segurança, elas não são, necessariamente, pensadas para que os dados pessoais estejam sendo tratados da forma mais adequada e nem sempre deixam claro e nem exigem para o usuário os procedimentos de segurança da informação mais adequados, como senhas fortes, segundo fator de autenticação e orienta comportamentos não arriscados.

Uma alternativa é, partindo da ANPD, com parceria ou não, a criação e a consolidação na sociedade de ferramentas que apoiem o trabalho dessas iniciativas, baseados nos princípios da LGPD e entregando mais segurança jurídica para esses negócios, uma vez que estarão utilizando ferramentas pensadas a partir do conceito de,

- *privacy by design*;
- acessibilidade;
- código aberto (salvo partes sensíveis do algoritmo);
- auditabilidade;
- gratuidade;
- ampla divulgação.

Essas ferramentas também tiram a necessidade de custos com outros serviços que em maior ou menor nível oneram o caixa dessas pequenas iniciativas, além de entregar segurança da informação e segurança jurídica para operação.

Essa construção deve se basear nos seguintes artigos e incisos:

- Art. 5º Para os fins desta Lei, considera-se:
  - III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
  - XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
  - VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

- § 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.
- § 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.

- Art. 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.
  - § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.
  - § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:
    - III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
  - § 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.
- 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.
- Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.

Segue uma tabela com exemplos práticos de outros países.

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

País	Ferramenta	Descrição	Impacto
França	CNIL Privacy Tools	Ferramentas de conformidade e guias práticos oferecidos pela CNIL, incluindo modelos de políticas e relatórios de incidentes.	Ajuda empresas francesas a implementarem políticas robustas de proteção de dados e evitarem penalidades.
Reino Unido	ICO Data Protection Portal	Portal de proteção de dados com orientações detalhadas sobre conformidade com a GDPR, incluindo templates e registros de impacto de privacidade.	Guia empresas do Reino Unido na conformidade com a GDPR, reduzindo riscos legais e operacionais.
Canadá	Privacy Toolkit for Businesses	Kit de ferramentas para pequenas e médias empresas, incluindo checklists de conformidade e exemplos de políticas de privacidade.	Aumenta a transparência e a conformidade das empresas com regras de privacidade.
Austrália	Privacy Management Plan Template	Modelo de plano de gestão de privacidade que inclui resposta a incidentes e avaliação de impacto conforme a lei de privacidade australiana.	Ajuda empresas a documentar políticas de privacidade e garantir segurança de dados pessoais.

Estados Unidos	NIST Privacy Framework	Estrutura técnica e operacional gratuita para gerenciamento de riscos de privacidade, desenvolvida pelo Instituto Nacional de Padrões e Tecnologia (NIST).	Guia empresas no gerenciamento de riscos de privacidade e na estruturação de seus programas internos.
Finlândia	MyData Operator Model	Padrões técnicos para operadores de dados pessoais, promovendo governança ética e transparência na gestão de informações pessoais.	Oferece uma infraestrutura de governança de dados mais ética e transparente.

Links

França: https://www.cnil.fr/en/gdpr-toolkit
Reino Unido: https://ico.org.uk/for-organisations/advice-for-small-organisations/create-your-own-privacy-notice/
Canadá: https://publications.gc.ca/site/eng/9.825788/publication.html
Austrália: https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/privacy-management-plan-template
Estados Unidos: https://www.nist.gov/privacy-framework
Finlândia: https://mydata.org/publication/understanding-mydata-operators/

3. Escore de Crédito

Um fator que se relaciona diretamente às condições de financiamento desses negócios é a capacidade de tomar crédito, as instituições financeiras exercem papel central na disponibilização ou não e em quais condições esse produto financeiro chega até o tomador do crédito. Essas condições dizem respeito ao valor total do crédito, os juros, a quantidade de parcelas, as taxas, entre outras. Para esses empreendedores que

necessitam urgentemente de dinheiro para "girar o caixa", tomar um crédito significa uma melhora direta nas condições de trabalho e expansão de seus negócios, gerando mais empregos, oportunidade de renda, desenvolvimento econômico, tecnológico e inovação. O artigo 7° no inciso X atesta a proteção ao crédito como uma hipótese legal,

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

O escore de crédito tem um papel decisivo na tomada de decisão das instituições financeiras em não conceder crédito, conceder e em quais condições se darão essa concessão. Esse escore, como qualquer outro escore, é um modelo estatístico que leva em consideração algumas informações para criar uma "régua" partindo de algumas premissas, essas premissas são os parâmetros do modelo, que por sua vez são os dados pessoais dos titulares de dados, seja de comportamento com seus compromissos financeiros, seja outros diversos dados pessoais sensíveis ou não.

Hoje não há uma clareza das informações pessoais que estão circulando pelas empresas controladoras e operadoras do processamento de escore de crédito, não é possível contestar ou ter acesso a todos os seus dados que foram considerados. Alguma base legal como a de crédito e o legítimo interesse, podem legitimar a utilização dos dados para o processamento, mas não justifica a falta de transparência, livre acesso, exclusão, entre outros princípios.

Baseado no Art. 20 da LGPD temos,

Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.
§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.
§ 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

Um dos princípios assegurados no artigo 6º da Lei Geral de Proteção de Dados Pessoais é o da não discriminação, que garante a "impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos". Por conseguinte, o artigo 5º define que o dado pessoal sobre origem racial ou étnica, convicção

religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural é considerado dado pessoal sensível, tendo tratamento especial pela lei e dependendo de consentimento expresso do titular, ressalvadas algumas hipóteses específicas elencadas nos artigos 11 a 13. Há ainda o artigo 20 (como já citado) que dá ao titular do dado pessoal o direito a solicitar a revisão de decisões de crédito e de consumo tomadas com base em "tratamento automatizado de dados pessoais". Em suma, ao garantir ao cidadão amplo acesso aos dados, e o direito de revisão de decisões de crédito automatizadas, a LGPD impõe às empresas um maior rigor e cautela em seu processo de análise de crédito e formação de credit score, que não poderá mais ser definido com base em dados de cunho discriminatório e nem com base em dados pessoais sensíveis.

As empresas que desenvolvem e vendem serviços de escores e as instituições financeiras que desenvolvem seus próprios escores e/ou consomem de um terceiro, podem e devem disponibilizar acesso facilitado, claro, compreensível e comunicar aos titulares de dados de forma proativa como esse dados pessoais foram utilizados. Baseado nos princípios da LGPD, esse estudo sugere a Política Nacional de Proteção de dados, que os controladores, operadores e clientes desses produtos de escore disponibilizem:

- Portal de acesso com
    - dados do titular processados para a geração de cada escore, tanto os de comportamento financeiro em outras instituições, dados esses que o Banco Central disponibiliza, quanto qualquer outro dado pessoal envolvido;
    - o peso de cada um desses dados, ou seja, como cada informação favorece ou desfavorece a avaliação daquela tomada de produto financeiro, uma vez que esse processo é automatizado e carece de transparência;
    - meios de atualização e exclusão de dados pelo titular, além de justificativas da existência de cada um desses dados em sua base.
- Histórico do comportamento de crédito utilizado para o próximo processamento do escore de crédito de forma atualizada no momento da consulta do titular de dados;
- Comunicar o titular de dados todas as vezes que um novo dado bancário ou não é disponibilizado na base de dados.

O comprimento das exigências da LGPD é um vetor de segurança jurídica importante para os controladores e operadores do escore de crédito, evitando qualquer não garantia de direitos à sociedade brasileira.

REFERÊNCIAS BIBLIOGRÁFICAS

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

BRIA, Francesca. **A cidade inteligente: tecnologias urbanas e democracia.** São Paulo: Ubu Editora, 2019.

SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS – SERPRO. **A LGPD impactará quem cede e quem pede empréstimos?**. Disponível em: https://www.serpro.gov.br/lgpd/noticias/lgpd-protecao-dados-pessoais-emprestimo-impacto#:~:text=Em%20suma%2C%20ao%20garantir%20ao,cunho%20discriminat%C3%B3rio%20e%20nem%20com. Acesso em: 8 dez. 2024.

DEPS. **Quais os efeitos da LGPD na análise de crédito? 3 passos importantes.** Disponível em: https://deps.com.br/quais-os-efeitos-da-lgpd-na-analise-de-credito-3-passos-importantes/. Acesso em: 8 dez. 2024.

JUSBRASIL. **Scoring de crédito é legal, mas informações sensíveis, excessivas ou incorretas geram dano moral**. Disponível em: https://conteudojuridico.com.br/consulta/artigos/58717/a-falta-de-transparncia-na-prtica-do-score-uma-anlise-luz-do-cdc-e-da-cr-88. Acesso em: 11 dez. 2024.

CONTEÚDO JURÍDICO. **A falta de transparência na prática do score: uma análise à luz do CDC e da CR/88.** Disponível em: https://conteudojuridico.com.br/consulta/artigos/58717/a-falta-de-transparncia-na-prtica-do-score-uma-anlise-luz-do-cdc-e-da-cr-88. Acesso em: 11 dez. 2024.

SERASA EXPERIAN. **Política de Transparência de Uso e Coleta de Dados - Cadastro Positivo. Disponível em**: https://www.serasaexperian.com.br/politica-de-transparencia-de-uso-e-coleta-de-dados-cadastro-positivo/. Acesso em: 11 dez. 2024.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANEXO XXIII – ESTUDO DE CASO: EDUCAÇÃO E INCLUSÃO

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ESTUDO DE CASO: EDUCAÇÃO E INCLUSÃO

por Isabella Henriques

Introdução

O avanço das tecnologias digitais tem transformado profunda e desigualmente diversos setores, incluindo a educação. Nesse contexto, a Inteligência Artificial desempenha um papel fulcral, com aplicações que vão desde a personalização do aprendizado até a otimização de processos administrativos. No entanto, esses avanços também trazem desafios significativos relacionados à proteção de dados e à privacidade, à acessibilidade e à inclusão, especialmente quando tecnologias como o reconhecimento facial são implementadas em ambientes escolares frequentados por crianças e adolescentes.

Assim, o presente estudo de caso pretende abordar algumas das inúmeras consequências dessas inovações sob múltiplas perspectivas, incluindo práticas nacionais e internacionais de proteção de dados e privacidade, conformidade legal, ética no uso de tecnologias e estratégias para evitar a ampliação de desigualdades.

Também apresenta alguns casos práticos, diretrizes e recomendações para o uso responsável dessas ferramentas, garantindo que tecnologias educacionais sejam utilizadas de maneira ética e que respeitem direitos fundamentais como a privacidade e a equidade. Essa análise se faz especialmente relevante em um cenário global onde a digitalização da educação vem sendo acelerada, ampliando oportunidades de aprendizado, mas também expondo crianças e adolescentes a práticas de vigilância e exploração de dados. A compreensão desses aspectos é essencial para o desenvolvimento de políticas públicas e diretrizes que promovam um uso seguro, ético e inclusivo das novas tecnologias digitais na educação, especialmente para grupos em situação de vulnerabilidade.

Ainda, vale uma ressalva inicial acerca do objeto deste compilado. Isso porque uma outra perspectiva para o tema da educação e inclusão diz respeito à necessidade de educação de todas as pessoas e também de crianças e adolescentes para a nova disciplina da proteção de dados e privacidade, no sentido de que todas as múltiplas infâncias e adolescências tenham mais informações e constituam conhecimento acerca do tema, que é tão relevante para suas vidas e que pode impactar essas pessoas sobremaneira. Assim, considerando a existência de um Grupo de Trabalho focado nessa temática (CNPD GT1), o presente estudo de caso concentrou-se nos usos de novas tecnologias nas escolas, deixando a educação em direitos para os trabalhos do GT1.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

(1) Reconhecimento facial nas escolas

O relatório do InternetLab ("Tecnologias de vigilância e educação: um mapeamento das políticas de reconhecimento facial em escolas públicas brasileiras"), lançado em março de 2023, faz um mapeamento do grau de expansão, formas de uso e práticas adotadas no uso dessas tecnologias em 15 escolas públicas de diferentes regiões do país. Entre os principais achados do relatório, ressalta-se:

Foram identificadas três finalidades principais para implementar o reconhecimento facial:

- (i) otimização da gestão do ambiente escolar (economia de tempo de aula dos professores, administrar as faltas escolares, gestão de merendas e material escolar)
- (ii) combate à evasão escolar (evitar alterações indevidas no registro de presença, comunicar o Conselho Tutelar e gerenciar programas sociais, em caso de muitas ausências);
- (iii) otimizar segurança (evitar que estudantes saiam sem autorização e proteger o patrimônio escolar)

Dessa forma, o reconhecimento facial nas escolas combateria, principalmente:

- (i) Superlotação das salas de aula;
- (ii) Falta de verbas para alimentação escolar
- (iii) Evasão escolar;
- (iv) Violência.

Apesar de auxiliarem no combate de problemas legítimos, análises sobre os casos de contestação e entrevistas com representantes da sociedade civil demonstram que essa tecnologia de reconhecimento **não combate, de forma eficiente, os problemas a que é endereçada**.

O relatório também destaca que o reconhecimento facial não é uma tecnologia propriamente da educação, mas uma **tecnologia de vigilância**. Seu uso tem sido criticado internacionalmente em função de denúncias sobre:

- Viés discriminatório;

- Questões relacionadas à segurança, transparência e eficácia do sistema.

No caso de escolas, cujo público são crianças e adolescentes, aumenta-se a sensibilidade do tópico e os perigos envolvidos. O relatório, por fim, estabelece algumas bases interessantes para orientar a adoção de tecnologias no ambiente escolar de forma geral, abaixo transcritas:

- "(i) Capacitação de gestores públicos para diferenciar os diferentes tipos de ferramentas tecnológicas;
- (ii) Análise de contexto: produção de análise prévia e de relatórios de impacto à proteção de dados, aos direitos humanos, dando ênfase aos potenciais discriminatórios que podem estar contidos no uso de tecnologias específicas;
- (iii) Participação e gestão democrática: cooperação entre diferentes setores da sociedade, com participação de corpos docente e discente;
- Aprimoramento dos mecanismos de transparência: respostas céleres e completas aos pedidos de LAI, divulgação de Política de Privacidade;
- (iv) Uso de software livre;
- (v) Capacitação e letramento digital e tecnológico para gestores públicos e para educadores(as)."

No contexto internacional, vale citar os estudos desenvolvidos pela área de pesquisa *Science, Technology and Public Policy* da Universidade de Michigan sobre 'Facial Recognition in Schools'. Apesar de o reconhecimento facial ser apontado como um meio eficiente e preciso de verificação da identidade, segundo os estudos, os perigos que essa tecnologia traz superariam seus supostos benefícios: *"a growing body of evidence suggests that it will erode individual privacy and disproportionately burden people of color, women, people with disabilities, and trans and gender non-conforming people"*. Em outras palavras, os estudos apontam que há um corpo de evidências crescente em relação à erosão da privacidade individual e ao aumento da discriminação sobre grupos sociais vulnerabilizados.

Importante também mencionar o relatório do Escritório de Serviços de Tecnologia da Informação da cidade de Nova Iorque, sobre o uso de biometria e outras formas de identificação nas escolas: 'Use of Biometric Identifying Technology in Schools'. De acordo com o documento, os riscos na utilização de reconhecimento

facial nas escolas são maiores do que os benefícios, mas provavelmente já há menos riscos para o uso estritamente administrativo dessa tecnologia. No entanto, também menciona o uso de identificação por impressões digitais como uma alternativa viável, com menos riscos.

(2) Uso da imagem no contexto educacional

A organização National Education Union (NEU), do Reino Unido, estabelece diretrizes interessantes para orientar o tratamento de imagens nas escolas no seu 'Photographs in schools':

- (i) Os materiais de imagem (fotografias ou vídeos) devem ser usados para os propósitos internos da escola;
- (ii) O uso dos materiais para qualquer propósito diverso deve buscar o consentimento dos sujeitos presentes nas imagens;
- (iii) O compartilhamento da imagem por pessoas fotógrafas com quaisquer terceiros apenas deve ocorrer quando houver especificação contratual para tal ou quando houver permissão pela escola;
- (iv) O fotógrafo deve reter evidências relativas ao atendimento dessas regras.

No caso de imagens utilizadas para propósitos de segurança, deve-se assegurar que:

- (i) Mães, pais ou tutores devem ser informados da retenção de imagens para propósito de segurança;
- (ii) As imagens devem ser armazenadas com segurança e usadas apenas por aqueles autorizados para tal.

Caso as imagens sejam utilizadas para fins publicitários, como no site da escola, a NEU orienta que o nome dos estudantes presentes nas imagens não seja divulgado. Caso haja intenção de atrelar a imagem ao nome do estudante (como no caso de fazer materiais sobre os melhores alunos, por exemplo) é necessário haver consentimento orientado pelas seguintes informações:

- (i) A identificação do controlador dos dados;
- (ii) O(s) propósito(s) para uso das imagens;

- (iii) A identificação de quaisquer organizações para as quais as imagens podem ser distribuídas;
- (iv) Quando as imagens serão eliminadas.

Em relação a fotografias e vídeos feitos por mães e pais de estudantes em eventos escolares, a orientação é que:

- (i) Seja incluída uma seção no contrato de matrícula indicando que qualquer imagem dos eventos escolares não será usada inapropriadamente;
- (ii) Seja incluído um termo assinável nas correspondências de convite a tais eventos, reafirmando que as imagens não serão usadas de maneira indevida;
- (iii) Haja confirmação escrita de que as imagens só serão feitas no local e horário do evento escolar;
- (iv) Seja informado onde a escola possui seu próprio registro fotográfico dos eventos.

(3) Uso das imagens em tecnologias educacionais

Há tecnologias dedicadas ao processo de ensino-aprendizagem que podem, eventualmente, registrar imagens dos estudantes. No caso do Reino Unido, o sistema IRIS Connect é dedicado para que professores gravem suas aulas com o fim de assisti-las e otimizá-las, além de compartilhar com colegas para feedbacks. Nesse contexto é imprescindível que:

- (i) A tecnologia seja segura e não permita reprodução do material por professor/a ou mediante sua permissão;
- (ii) Os alunos sejam avisados da gravação e dos termos de visualização e compartilhamento
- (iii) O acesso à biblioteca de gravações por outras pessoas possa ser revogado a qualquer tempo.

Os AV1 Robots, por sua vez, são uma tecnologia assistiva destinada àqueles que não podem comparecer presencialmente às aulas, no caso por exemplo de problemas de saúde crônicos. Apesar de os AV1 Robots apenas permitirem a transmissão das aulas, e não sua gravação, é importante lembrar que as pessoas usuárias desse serviço podem gravar o conteúdo por meio de outro *software*. Por isso, é importante que haja um termo

de uso a ser assinado pelo estudante ou por seus tutores, com o compromisso de não realizarem esse ou qualquer uso indevido.

Em relação ao posicionamento da NEU sobre as tecnologias da inovação nas escolas, vale mencionar o trecho abaixo (tradução livre):

> "*A NEU não acredita que a utilização de tecnologia inovadora nas escolas seja intrinsecamente boa ou má. Salientamos, no entanto, a importância do consentimento informado e a necessidade de as escolas consultarem os pais, os alunos e o pessoal da escola/faculdade antes de introduzirem tecnologia potencialmente intrusiva deste tipo. Se os alunos e funcionários desejarem optar por não ter suas imagens e falas capturadas por esses dispositivos, eles deverão poder fazê-lo.*"

(4) Educação, Inteligência Artificial e proteção de dados

As diretrizes para coleta e tratamento de dados no contexto educacional devem levar também em consideração o uso de tecnologias de Inteligência Artificial. A partir do surgimento e disseminação dessas novas tecnologias, cada vez mais informações são coletadas e processadas.

É o caso, por exemplo, das tecnologias de análise de linguagem no contexto educacional. São capazes de gerar diagnósticos e promover melhorias no processo de ensino-aprendizagem. A partir da análise da proficiência linguística dos estudantes e de seus padrões de expressão, o processo se torna mais personalizável e subjetivo, adequado a atender as necessidades individuais de cada estudante.

Estudo da Strathmore University, sobre privacidade de dados e plataformas ed-tech do continente africano '[Data Privacy in Africa's Ed-Tech Platforms: Children's Right to Privacy]', traz outro caso prático de aplicação de Inteligência Artificial no processo de ensino-aprendizagem e aponta também as deficiências relacionadas às políticas de privacidade:

- Só 11 das 22 plataformas analisadas (aplicações baseadas no Oeste e Sul do continente africano) têm políticas de privacidade. E apenas 4 mencionam crianças e seus direitos e se/como os tutores podem participar ativamente pelo consentimento;
- As outras 11 não possuem políticas de privacidade nem após o registro;

- À exceção do Nigerian Data Protection Regulation, que prevê especificamente sobre política de privacidade, os outros frameworks de proteção de dados na África têm apenas componentes de uma política de privacidade, e não uma política estruturada.

O documento faz uma série de recomendações para desenvolver as políticas de proteção de dados de Ed-Techs que utilizam IA; também satisfazendo a necessidade de abordar especificamente a proteção de dados de crianças:

- Inclusão de uma seção de coleta de dados que inclua informações sobre o tipo de informação coletada de crianças e maneira da coleta. Deve especificar se a coleta é por meio de áudio, vídeo ou outros formatos.
- Inclusão de uma cláusula de comunicação, detalhando se o responsável pela plataforma pretende enviar correspondências e a maneira como isso será feito. A criança e seus responsáveis devem ser informados de qualquer comunicação que podem receber.
- Lista detalhada de todos aqueles que têm acesso aos dados da criança, como tutores, pais, donos da plataforma, organizações externas, etc., e se possível como usarão os dados acessados.
- Pronunciamento claro e facilmente acessível detalhando os direitos daqueles legalmente definidos como crianças. Deve incluir informação sobre o direito de retirada dos dados da plataforma, direito de revogar o consentimento, direito de requisitar exclusão dos dados, direito de requisitar acesso à suas informações.
- Pronunciamento afirmando que a plataforma não coleta informações identificáveis das crianças. Deve afirmar categoricamente que a criança não receberá pedidos de dar informações de contato ou qualquer outra informação que possa ser usada para identificá-la.
- Pronunciamento afirmando claramente os requisitos para consentimento dos pais ou responsáveis (como definido de acordo com a lei do país). Deve informar também como pais ou responsáveis podem entrar em contato com a plataforma para remoção dos dados da criança, especialmente quando forem coletados sem consentimento. Deve-se afirmar também que as interações entre tutor e criança ocorrerão sempre em ambiente supervisionado (inclusive sessões privadas).

- Inclusão de uma sessão informando os usuários sobre a existência de terceiros afiliados e detalhando os protocolos da plataforma sobre possível compartilhamento de informações com essa parte. Deve detalhar quais informações podem ser compartilhadas e em que quantidade.

- Inclusão de um pronunciamento detalhando as leis de proteção de dados aplicáveis. Além disso, deve mencionar as estruturas protetivas que definem o conceito de criança e seu direito à privacidade.

Outro exemplo é a exploração comercial de crianças e adolescentes no âmbito do tratamento de seus dados estudantis. Relatório de pesquisa da Iniciativa Educação Aberta, publicado em 2020[167], a esse respeito, comprovou uma série de abusos nos Termos de Uso das plataformas educacionais disponibilizadas no Brasil por empresas de tecnologia. É importante que se diga que não consentir com os termos de uso e políticas de privacidade das empresas de tecnologia nem sempre é uma opção real para a maioria dos estudantes, como aconteceu, por exemplo, no contexto de aprendizado remoto durante a pandemia de Covid-19.

Caso emblemático, acerca dos riscos da IA na educação, foi também a utilização, pelo governo do Reino Unido, de um algoritmo para a classificação das notas dos estudantes que fariam o exame nacional, então cancelado em virtude da pandemia de Covid-19. Como posteriormente restou comprovado, o algoritmo prejudicou estudantes de comunidades e bairros mais vulneráveis e favoreceu aqueles das escolas localizadas em comunidades e bairros mais privilegiados, ampliando, assim, as iniquidades já existentes.[168]

Sistemas de IA usados em escolas podem ser voltados aos estudantes, aos professores e ao sistema de ensino[169]. Sistemas de aprendizagem adaptativa voltados aos estudantes podem empregar algoritmos, avaliações, *feedbacks* dos alunos e várias mídias para fornecer material personalizado às necessidades e ao

[167] GONSALES, Priscila; TEL, Amiel. Educação, Dados e Plataformas: Análise descritiva dos termos de uso dos serviços educacionais Google e Microsoft. Disponível em: https://aberta.org.br/educacao-dados-e-plataformas/ (Acesso em: 9 Dez 2024).

[168] SATARIANO, Adam. British grading debacle shows pitfalls of automating government: The uproar over an algorithm that lowered the grades of 40 percent of students is a sign of battles to come regarding the use of technology in public services. The New York Times, 2020. Disponível em: https://www.nytimes.com/2020/08/20/world/europe/uk-england-grading-algorithm.html (Acesso em: 9 Dez 2024).

[169] UNITED NATIONS CHILDREN´S FUND (UNICEF); UC BERKELEY HUMAN RIGHTS CENTER RESEARCH TEAM. Executive Summary: Artificial Intelligence and Children´s Rights. Disponível em: https://www.unicef.org/innovation/media/10726/file/Executive%20Summary:%20Memorandum%20on%20Artificial%20Intelligence%20and%20Child%20Rights.pdf (Acesso em: 9 Dez 2024).

progresso de cada estudante[170], sendo que a IA pode ser usada para melhorar as habilidades sociais, especialmente das crianças com deficiência[171]. Também os robôs educacionais prometem benefícios para as crianças, como ensino personalizado, desenvolvimento de habilidades sociais e educação à distância para quem necessita – ainda que até hoje não haja comprovação alguma de sucesso nessa seara. Já a IA voltada à categoria dos professores pode apoiá-los nas tarefas de correção de trabalhos, detecção de plágio e otimização do tempo junto aos estudantes.

De qualquer forma, é praticamente um consenso que o debate sobre a tecnologia educacional deve sair do "se" e evoluir para o "como", na medida em que não mais se deve discutir se a tecnologia deve estar na escola, mas 'como' isso deve acontecer. Relevante pesquisa sobre o tema, liderada pelo professor Paulo Blikstein[172], aponta para quatro dimensões: (i) recursos e infraestrutura; (ii) pessoas: profissionais e formação; (iii) segurança de dados pessoais na educação; (iv) estratégia nacional. Assevera, ainda, que os vários tipos de tecnologia educacional podem ser divididos em três categorias: infraestrutura, ensino e criação/ experimentação.

A propósito da proteção de dados estudantis e da privacidade de crianças e adolescentes na educação, o Instituto Alana, juntamente com EducaDigital, Intervozes e Nic.Br, elaborou o material 'A escola no mundo digital – Um guia sobre proteção de crianças e adolescentes no uso de tecnologias nas escolas' que aborda o tema sob as múltiplas discussões. Trata-se de um material para famílias, educadores e gestores escolares, mas, sinteticamente, aborda as questões mais contemporâneas sobre o tema e pode apoiar na elaboração de guia de boas práticas sobre o tema.

---

[170] Exemplo do uso de Intelgiência Artificial customizado para estudantes é o aplicativo Duolingo para o aprendizado de idiomas. SNOW, Jackie. AI Technology is disrupting the traditional classroom. Here's a progress report. – Artificial Intelligence has the potential to personalize learning at scale. The challenge: making sure it benefits everyone. Nova Iorque, 2019. Disponível em: https://www.pbs.org/wgbh/nova/article/ai-technology-is-disrupting-the-traditional-classroom/ (Acesso em: 9 Dez 2024).

[171] Exemplo desse uso pode ser verificado nos produtos da empresa Brain Power. BRAIN POWER. Disponível em: https://www.brain-power.com (Acesso em: 9 Dez 2024).

[172] BLIKSTEIN, Paulo; BARBOSA E SILVA, Rodrigo; CAMPOS, Fabio; MACEDO, Lívia. Tecnologias para uma educação com equidade: Novo horizonte para o Brasil. Relatório de política educacional. Brasília: Todos pela educação; Dados para um debate democrático; Tranformative Learning Technologies Lab, 2021. Disponível em: https://todospelaeducacao.org.br/wordpress/wp-content/uploads/2021/04/Relatorio-Tecnologias-para-uma-Educacao-com-equidade.pdf?utm_source=site (Acesso em: 9 Dez 2024).

(5) Estudantes, não produtos

Relatório da Human Rights Watch (HRW) divulgado em maio de 2022 revelou que a maioria dos produtos de tecnologia educacional endossados por governos em 49 países durante a pandemia de Covid-19 violou ou colocou em risco os direitos de crianças e adolescentes. Dos 163 produtos analisados, 145 (89%) realizaram vigilância ou tinham a capacidade de vigiar estudantes, muitas vezes sem o consentimento ou conhecimento deles ou de suas famílias:

- Coleta de Dados em Larga Escala: Muitos produtos de EdTech coletaram informações pessoais, incluindo identidade, localização, atividades online, conexões familiares e amigos, e dados sobre os dispositivos utilizados pelos estudantes. Essas práticas ocorreram fora do horário escolar, invadindo a privacidade das crianças e mergulhando em detalhes de suas vidas privadas.

- Falta de Transparência: crianças, pais e professores desconheciam as práticas de coleta de dados desses produtos. A maioria dos sistemas de EdTech analisados não oferecia aos estudantes a possibilidade de recusar a vigilância sem abandonar o ensino online.

- Responsabilidade dos governos: 39 dos 42 governos que desenvolveram seus próprios sistemas de aprendizagem online violaram ou colocaram em risco os direitos das crianças e adolescentes ao coletar dados pessoais de maneira inadequada. Poucos governos avaliaram se os produtos EdTech endossados eram seguros para uso infantil.

- Impactos na Educação: a vigilância era praticamente inevitável para os estudantes, exceto se optassem por renunciar à educação formal durante a pandemia.

As recomendações desse estudo passam pelos seguintes pontos:

- Adoção de Leis de Proteção de Dados: os governos devem implementar e aplicar legislações modernas que protejam os dados de crianças e adolescentes. Essas leis devem impedir que empresas priorizem interesses comerciais acima da privacidade e segurança dos estudantes.
- Transparência e Consentimento: governos e empresas devem garantir que práticas de coleta de dados sejam claras, acessíveis e realizadas com o consentimento explícito dos responsáveis legais.

Ferramentas educacionais devem oferecer opções que permitam aos estudantes participar sem serem monitorados.

- **Campanha Global de Conscientização**: a HRW lançou a campanha #StudentsNotProducts (#EstudantesNãoProdutos), envolvendo famílias, educadores e aliados na luta por maior proteção online para crianças e adolescentes.
- **Responsabilidade Corporativa:** empresas devem reformular suas práticas para colocar os interesses das crianças acima dos objetivos comerciais, adotando medidas éticas para lidar com dados pessoais.
- **Fiscalização Governamental:** é essencial que os governos realizem auditorias regulares em plataformas EdTech para garantir conformidade com padrões de privacidade e segurança.

Como conclusão, o relatório destaca a urgência de proteger crianças e adolescentes de práticas abusivas no ambiente digital educacional, no sentido de que governos e empresas repensem suas abordagens, priorizando a proteção de dados e a privacidade e os direitos de crianças e adolescentes como base para qualquer iniciativa tecnológica educacional. A conscientização pública e ações concretas são, de fato, fundamentais para evitar que estudantes sejam tratados como produtos em um mercado de dados.

Essa vigilância constante e intrusiva pode comprometer não só o presente, mas o futuro das crianças, no sentido de terem oportunidades ameaçadas por instituições que as julguem em razão de dados relacionados, como, por exemplo, informações de saúde, capacidades intelectuais e mesmo comportamento. O excesso de vigilância também pode afetar negativamente a sua constituição socioemocional, tirando-lhes o impulso da experimentação e do aprendizado por meio dos erros:

> "(...) vigilância demais pode violar o espírito das pessoas. Educar crianças sob vigilância é criar súditos, não cidadãos. E nós queremos cidadãos. Para seu próprio bem-estar e para o bem da sociedade.
> A sociedade precisa de cidadãos autônomos e engajados, capazes de questionar e transformar o *status quo*. Os grandes países não são formados por seguidores servis. Para se tornarem pessoas com corações e mentes fortes, as crianças precisam explorar o mundo, cometer erros e aprender com a própria experiência, sabendo que os erros não serão registrados, muito menos usados contra elas. A privacidade é necessária para cultivar a intrepidez." [173]

[173] VÉLIZ, Carissa. Privacidade é poder: Por que e como você deveria retomar o controle de seus dados. Tradução Samuel Oliveira. 1a Edição. São Paulo: Editora Contracorrente, 2021, pp. 208-209.

Nesse sentido, de fato, os ensinamentos da professora Carissa Véliz seguem mais atuais do que nunca para essa discussão:

> "É um mundo em que você se preocupa com a privacidade de seus filhos. Você se pergunta se o futuro deles pode estar comprometido quando jogam jogos online, pois você sabe que as pontuações deles são vendidas a corretores de dados que calculam as capacidades cognitivas. Você se preocupa que eles possam errar, como ficar bêbados na adolescência e serem fotografados, e que por causa disso eles nunca consigam um emprego. Você se preocupa com o quanto eles têm de ser obedientes para ter uma chance de serem bem-sucedidos na sociedade. Você se preocupa com o fato deles nunca sentirem o gosto da liberdade. Esta é uma sociedade preparada para uma tomada de poder autoritária." [174]

(6) IA, Educação, Acessibilidade e Inclusão

A aplicação de Inteligência Artificial na educação tem potencial para reduzir barreiras de acesso ao aprendizado e promover inclusão. No entanto, é essencial que as soluções sejam projetadas com foco em diversidade, equidade e acessibilidade, de forma a atender às necessidades de todos os estudantes, incluindo aqueles em situações de vulnerabilidade ou com deficiências.

IA para Educação Inclusiva: permite personalizar o aprendizado para atender a diferentes estilos, ritmos e necessidades de aprendizagem. Ferramentas baseadas em IA têm demonstrado eficácia na personalização do conteúdo e apoio a estudantes com deficiências. Ferramentas de IA fornecem suporte para:

- **Deficiências visuais**: *softwares* como o Microsoft Seeing AI usam visão computacional para descrever imagens e textos.
- **Deficiências auditivas**: aplicativos como o Google Live Transcribe convertem áudio em texto em tempo real, permitindo que estudantes surdos ou com deficiência auditiva acompanhem aulas.
- **Deficiências cognitivas**: ferramentas que simplificam a linguagem ou organizam informações, como assistentes virtuais baseados em IA, podem auxiliar estudantes com dificuldades de aprendizado.

Promoção de Diversidade Linguística: em contextos multilíngues, a IA permite a tradução e a personalização de conteúdos para estudantes que falam diferentes idiomas. Ferramentas como o Google

[174] VÉLIZ, Carissa. Privacidade é poder: Por que e como você deveria retomar o controle de seus dados. Tradução Samuel Oliveira. 1a Edição. São Paulo: Editora Contracorrente, 2021, p. 260.

Translate e o Duolingo demonstram como tecnologias baseadas em IA podem superar barreiras linguísticas e ajudar no aprendizado de línguas. Em ambientes multiculturais, algoritmos devem ser treinados para respeitar nuances culturais e evitar vieses que marginalizam grupos minoritários.

Design Universal e Acessibilidade: as soluções baseadas em IA devem seguir os princípios do Desenho Universal para Aprendizagem (DUA), que incluem:

- Representação múltipla: apresentar informações de maneiras diversas, como texto, áudio, imagens ou vídeo, para atender diferentes estilos de aprendizagem.
- Ação e expressão múltiplas: permitir que estudantes interajam e demonstrem seu aprendizado de várias formas.
- Engajamento múltiplo: criar ferramentas que mantenham os alunos motivados, respeitando suas preferências individuais.

Alguns dos desafios e das preocupações éticas incluem:

- Vieses algorítmicos: podem reforçar preconceitos se forem treinados com dados desbalanceados. Isso pode afetar negativamente estudantes de grupos marginalizados.
- Desigualdade digital: muitos estudantes ainda não têm acesso a dispositivos ou internet de qualidade, limitando os benefícios da IA.
- Privacidade e proteção de dados: ferramentas de IA na educação devem priorizar a segurança dos dados de estudantes, especialmente em contextos de vulnerabilidade.

Sobre o tema, já existem diretrizes internacionais tais quais as seguintes:

- UNESCO: o relatório 'Artificial Intelligence in Education: Challenges and Opportunities for Sustainable Development' destaca o papel da IA na promoção da inclusão e igualdade na educação. A UNESCO também recomenda a adoção de políticas que assegurem acessibilidade e inclusão para todos os estudantes.
- UNICEF: o documento 'Policy Guidance on AI for Children' sugere que soluções de IA sejam projetadas com foco nos direitos e nas necessidades das crianças, especialmente em situações de exclusão social.
- World Economic Forum (WEF): relatórios sobre o impacto da tecnologia na educação enfatizam o papel da IA em tornar o aprendizado mais acessível e equitativo.

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

(7) Considerações finais
Por fim, vale ressaltar:

(i) Com a interoperabilidade das tecnologias na atualidade, especialmente de IA, o treinamento ocorre simultaneamente via múltiplas fontes de dados. Não há como saber (ainda) se um *software* dito "do bem" com foco em apoiar uma demanda de inclusão não está também intercambiando dados para usos indevidos. A UFRJ fez um estudo de apps de saúde e bem estar, a imensa maioria intercambia com grandes empresas de tecnologia sem deixar isso claro a priori;

(ii) Seria importante mapear tecnologias alternativas, tecnologias cívicas, community tech e empresas alternativas que podem oferecer soluções para inclusão ou para atividades pedagógicas. Entender como operam, qual servidor ou infraestrutura utilizam, qual a base de dados, se seguem a LGPD e as demais normativas de proteção às infâncias e adolescências, se usam IA (qual técnica?), se intercambiam dados com grandes empresas de tecnologia ou não. Isso é importante não apenas para a questão de proteção de crianças e adolescentes como também para fomentar a inovação no país;

(iii) É ainda relevante entender como se dá o uso de dados nas diferentes aplicações para que se possa auditar melhor os riscos: imagens/fotografias, programação tradicional, IA simbólica (assistentes virtuais, tutores, avaliação por ex.) e IA conexionista (RF e IAGen estão nessa categoria).

(iv) Fundamental um olhar da ANPD especificamente para tecnologias que estão dentro da escola, associando proteção de dados com garantia do direito à educação, pois nem sempre quando os dados são protegidos se garante que não serão comercializados. A propósito, vale considerar o Parecer de Rafael Zanatta.

*****

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANEXO XXIV – ESTUDO DE CASO: CIDADES INTELIGENTES

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ESTUDO DE CASO: CIDADES INTELIGENTES

Conselheiro da ANPD: Rony Vainzof[175]

1. INTRODUÇÃO

1. Na era da quarta revolução industrial, um conjunto abrangente de tecnologias avançadas, como inteligência artificial, robótica, internet das coisas e computação em nuvem, estão transformando os métodos de produção e os modelos de negócios no Brasil e no mundo.[176] Desse contexto fazem parte as cidades inteligentes (cidades conectadas, ou *smart cities*, em inglês), que buscam a melhoria da qualidade de vida dos indivíduos nas cidades ao proporcionar mais eficiência, inclusão e sustentabilidade na prestação dos serviços urbanos.

2. Nesse ambiente de inovação tecnológica, os dados pessoais desempenham um papel fundamental. Eles não apenas alimentam as soluções tecnológicas implementadas nas cidades inteligentes, como também permitem que essas soluções sejam personalizadas e otimizadas para atender às necessidades reais das populações urbanas. A coleta, o processamento e o compartilhamento de dados, como padrões de mobilidade, consumo de energia e sustentabilidade, possibilitam avanços econômicos e tecnológicos significativos, impulsionando novos modelos de negócios e estimulando a inovação.

3. Por outro lado, o uso intensivo de dados pessoais em cidades inteligentes levanta questões cruciais sobre a privacidade e a proteção de dados. A confiança dos cidadãos é um pilar essencial para o sucesso dessas iniciativas, e o cumprimento de legislações como a Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil é indispensável para garantir que os direitos de liberdade fundamentais dos indivíduos sejam preservados. Assim, o equilíbrio entre o desenvolvimento tecnológico, a inovação e a proteção dos dados pessoais surge como um desafio estratégico para os gestores públicos, empresas e demais atores envolvidos no ecossistema das cidades inteligentes.

4. Este Estudo busca explorar como as cidades inteligentes podem alavancar o uso de dados pessoais para fomentar o desenvolvimento econômico, tecnológico e a inovação, ao mesmo tempo em que demonstra

[175] Conselheiro titular do CNPD. O trabalho contou com o apoio dos pesquisadores Verônica Barros e Mateus Lamonica.
[176] Disponível em: https://www.portaldaindustria.com.br/

formas de mitigar os desafios éticos e legais associados à privacidade, proteção de dados e à segurança da informação.

2. A IMPORTÂNCIA DO USO E DA PROTEÇÃO DE DADOS PESSOAIS EM CIDADES INTELIGENTES PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO RESPONSÁVEL.

5. No Brasil, há inúmeras iniciativas para estimular o desenvolvimento de cidades inteligentes, não apenas em termos de políticas públicas, como a Carta Brasileira para Cidades Inteligentes[177] - que possui um guia de implementação para os municípios com foco no desenvolvimento sustentável[178] -, mas também em propostas legislativas, com aplicabilidade nacional, como o caso do Projeto de Lei nº 976/2021, que tramita na Câmara dos Deputados[179] e que visa instituir a Política Nacional de Cidades Inteligentes (PNCI).

6. Segundo esse PL, cidades inteligentes são definidas como[180]: ***"espaço urbano orientado para o investimento em capital humano e social, o desenvolvimento econômico sustentável e o uso de tecnologias disponíveis para aprimorar e interconectar os serviços e a infraestrutura das cidades, de modo inclusivo, participativo, transparente e inovador, com foco na elevação da qualidade de vida e do bem-estar dos cidadãos."***

[177] Carta Brasileira para Cidades Inteligentes. *"A Carta é um pacto com conceitos, estratégias e recomendações para o estabelecimento de padrões de desenvolvimento urbano sustentável no Brasil, levando em conta os riscos e oportunidades da transformação digital nesse contexto. (...) É fruto da cooperação entre os governos do Brasil e da Alemanha para o Apoio à Agenda Nacional de Desenvolvimento Urbano Sustentável (Andus), um projeto da Coordenação-Geral de Apoio à Gestão Regional e Urbana do Ministério do Desenvolvimento Regional em parceria com a GIZ (Deutsche Gesellschaft für Internationale Zusammenarbeit), que conta com os apoios financeiro da Iniciativa Internacional de Proteção do Clima (IKI) e técnico-institucional do Ministério de Ciência, Tecnologia e Inovações (MCTI) e do Ministério das Comunicações (MCOM)."*

[178] Disponível em: https://cartacidadesinteligentes.org.br/guia/apresentacao

[179] Disponível em:https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1977843&filename=PL%20976/2021

[180]V. Artigo 2º II, do PL nº 976/2021 (Câmara dos Deputados);

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

7. A Autoridade Nacional de Proteção de Dados (ANPD) desenvolveu estudo sobre o tema[181] no qual apresentou as vantagens que as cidades inteligentes podem oferecer[182] e demonstrou as situações[183] nas quais dados, inclusive pessoais, são tratados[184]. Suas considerações estão resumidas abaixo:

- Qualidade de vida: serviços e infraestruturas mais acessíveis e eficientes, como transporte público melhorado, serviços de saúde eficazes e gestão otimizada de recursos naturais.
- Eficiência energética e sustentabilidade: sistemas inteligentes de iluminação, gestão de energia, uso de energias renováveis, otimização do uso da água e gestão de resíduos para promover a sustentabilidade ambiental.
- Mobilidade urbana: transporte com soluções inteligentes, como transporte público eficiente, compartilhamento de carros e informações em tempo real sobre o tráfego.
- Gerenciamento de recursos: tecnologias para monitorar e otimizar o uso de recursos, reduzindo desperdícios e custos operacionais.
- Participação cidadã: envolvimento da comunidade com plataformas digitais, permitindo que os cidadãos interajam com autoridades e participem da tomada de decisões.
- Segurança e resposta a emergências: infraestrutura inteligente e sistemas de monitoramento para melhorar a segurança pública, detectar incidentes e responder a emergências de forma mais eficiente.

8. Embora surjam preocupações, extremamente válidas e relevantes, no que toca à privacidade e segurança dos titulares de dados pessoais, a compatibilidade (através de medidas mitigadoras de riscos) entre o

[181] "Radar Tecnológico – Cidades Inteligentes, 2024." Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/publicacao_radar_tecnologico_jan_2024.pdf
[182] Segundo a OCDE (2020), *"cidades inteligentes são iniciativas ou abordagens que utilizam efetivamente a digitalização de forma a melhorar a qualidade de vida dos cidadãos e entregar serviços urbanos e ambientes mais eficientes, sustentáveis e inclusivos, como parte de um processo colaborativo envolvendo diversas partes interessadas."*
[183] Estudo preliminar sobre Cidades Inteligentes, 2024;
[184] Como bem assentou a ANPD, a Internet das Coisas[184] é uma infraestrutura fundamental, pois provê a capacidade de interconexão dos objetos de uso diário de capturar, processar, armazenar, transmitir e exibir informações, além de agir de forma autônoma e produzir dados em grande quantidade e diversidade exponencial, resultantes de suas interações.

desenvolvimento das cidades inteligentes e o tratamento de dados pessoais é admitida pela ANPD e evidenciada no PL acima mencionado[185].

9. Abaixo listamos projetos já implementados em cidades brasileiras no contexto de cidades inteligentes (ANPD, 2024):

Cidades	Iniciativas
Fortaleza (CE)	+ Implementação de GPS em ônibus para maior previsibilidade nos itinerários; + Projeto-piloto de partilha de carros elétricos através de IoT.
Águas de São Pedro (SP)	+ 500 sensores de estacionamento para informar, por meio de aplicativo, a disponibilidade de vagas nas principais vias do município; + Implantação de iluminação pública inteligente em um dos principais parques da cidade para controlar o estado das lâmpadas e sua operação; + Câmeras inteligentes de monitoramento das vias públicas, com geração de alarmes; + Solicitação online de consultas médicas; + Acesso biométrico dos usuários aos registros médicos e consultas, garantindo uma comunicação confidencial; + Dispositivos móveis nas escolas para alunos e professores
Rio de Janeiro (RJ)	+ Centro de Operações Rio (COR), fundado em 2010, integrando cerca de 30 agências da cidade que acessam dados de câmeras e sensores visando melhorar o trânsito e a gestão de emergências na cidade; + A região da Praça Mauá foi escolhida para as transformações do Programa de Inovação Social e Urbana de uma empresa multinacional de conectividade. Ele apresenta 15 soluções inteligentes desenvolvidas pela empresa e startups de tecnologia, e suas principais soluções em IoT incluem monitoramento da qualidade do ar, monitoramento e gerenciamento de bueiros e sensores de ruído

[185] "**Art. 4º** A cidade inteligente deverá ser regida pelos seguintes princípios: I – dignidade da pessoa humana;(...) V – privacidade dos cidadãos e segurança dos dados. **Art. 5º** O desenvolvimento de iniciativas de cidades inteligentes deverá observar as seguintes diretrizes: (...) X – estímulo ao desenvolvimento tecnológico, empreendedorismo e à inovação;(...) XIV – transparência e publicidade de dados e informações, sem prejuízo à privacidade da população e à segurança dos dados;"

Canoas (RS)	+ Implantação de mais de 30 sensores para detectar ruídos de alerta, como disparos de armas de fogo, que avisam automaticamente a Central Integrada de Monitoramento do Gabinete de Gestão Integrada Municipal.
Paulínia (SP)	+ Instalação de 25 estações de coleta de lixo na cidade, reduzindo até 30% os custos desse serviço.
São José dos Campos (SP)	+ Implantação de sensores climáticos e de detecção de disparos e de ruídos, por exemplo, para medir temperatura, umidade e níveis de CO_2. A cidade também se beneficiará: + de uma rede de Wi-Fi pública; + de um sistema de iluminação pública inteligente; + de um sistema de resposta de emergência, composto por 500 câmeras conectadas; + de sistemas de software e de 205 km de cabos de fibra ótica.
Itu (SP)	+ Implantação de um sistema inteligente de coleta de resíduos, com 3.300 contêineres distribuídos pela cidade.
Vitória (ES)	+ Implantação da Rede Bem-Estar, que interliga os equipamentos de saúde (unidades de saúde, pronto-atendimentos, farmácias, laboratórios, consultórios odontológicos, centros de referência e especialidades) em um único sistema; + Implantação do "Prontuário Eletrônico", software que oferece serviços como o de gestão de agendamento de retomo de consultas e a avaliação de atendimento via SMS.

10. Além desses casos, o *Ranking Connected Smart Cities* de 2023[186] mapeou mais de 600 municípios no Brasil, com mais de 50 mil habitantes, para apresentar as cidades mais inteligentes e conectadas. Segundo esse *Ranking*, o desenvolvimento das *smart cities* só é atingido quando os agentes de desenvolvimento da cidade compreendem o verdadeiro potencial da conectividade entre todos os setores, dando ênfase à importância do compartilhamento de dados nesse contexto.

11. Ademais, no estudo *IESE Cities in Motion Index* (IESE, 2022)[187], há menção de seis cidades brasileiras: São Paulo, na 130ª posição, seguida por Rio de Janeiro (136ª), Curitiba (153ª), Brasília (159ª), Salvador (169ª) e Belo Horizonte (172ª) (ANPD, 2024).

[186] Disponível em: https://web.nectainova.com.br/rcsc_ranking-csc_2024
[187] Disponível em: https://www.iese.edu/media/research/pdfs/ST-0633-E.pdf

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

2.1. O TRATAMENTO DE DADOS PESSOAIS NO CONTEXTO DAS CIDADES INTELIGENTES NAS DIVERSAS POLÍTICAS PÚLICAS NACIONAIS E NECESSIDADE DE HARMONIZAÇÃO NA PNPD

12. Além desses exemplos concretos já implementados em cidades brasileiras, diversas políticas públicas nacionais incentivam o desenvolvimento de cidades inteligentes, considerando-o como fundamental para o progresso econômico e tecnológico do país. Como os dados pessoais são imprescindíveis nesse contexto, é essencial que a Política Nacional de Proteção de Dados Pessoais e Privacidade reconheça essa relevância e busque harmonizar as iniciativas governamentais já existentes, convergindo esforços e orientando sobre o tratamento ético e responsável dos dados pessoais para o alcance de tal objetivo.

13. A seguir, detalhamos como esses temas são abordados nos planos de governo mais relevantes para o Brasil.

Estratégia Brasileira de Transformação Digital (E-Digital)[188]

14. A E-Digital busca impulsionar o desenvolvimento digital do Brasil, promovendo a inclusão digital, a inovação, a competitividade e o crescimento econômico sustentável. A estratégia se estrutura em dois eixos principais: Habilitadores e de Transformação Digital. Os Eixos Habilitadores focam em infraestrutura e acesso às TIC, pesquisa e desenvolvimento, confiança no ambiente digital, educação e capacitação profissional e dimensão internacional. Os Eixos de Transformação Digital visam transformar a economia e o governo, com foco na economia baseada em dados, dispositivos conectados, novos modelos de negócio, cidadania e governo digital. Destacamos algumas **ações estratégicas**:

- **Eixo Habilitador "C . Confiança no ambiente digital":** estas ações demonstram como a proteção de dados pessoais é um fator estruturante para atingir os objetivos de toda a estratégia de transformação digital.

[188] Criada originalmente em 2018, pela Portaria MCTIC nº 1.556/2018, a E-Digital foi atualizada para o período 2022-2026 e aprovada através da Portaria nº 6.543/2022, do Ministério da Ciência, Tecnologia e Inovação. Portanto, a E-Digital, permanece válida até sua próxima revisão. Ela surgiu como integrante do Sistema Nacional para a Transformação Digital, instituído pelo Decreto nº 9.319/2018, que trouxe a estrutura de governança para a implantação E-Digital. Este Decreto nº 9.319/2018 foi recentemente revogado pelo Decreto nº 12.308, de 11 de dezembro de 2024, que simplificou a estrutura governamental e manteve apenas o Comitê Interministerial para a Transformação Digital (CITDigital), com objetivo de assessorar o Presidente da República na elaboração, na implementação e no acompanhamento de políticas públicas destinadas à transformação digital. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosestrategiadigital/e-digital_ciclo_2022-2026.pdf.

- Fortalecer a cultura de proteção de dados pessoais: incentivar a prevenção de infrações à LGPD, capacitar agentes de tratamento e orientar a sociedade sobre normas de proteção de dados.
- Monitoramento contínuo: fiscalizar a aplicação da LGPD e propor melhores práticas e códigos de conduta.
- Conscientização sobre a LGPD: promover a aplicação da LGPD no setor público e privado, incluindo *startups* e pequenas empresas.
- Detecção e fiscalização: implementar mecanismos eficazes de monitoramento e fortalecer a ANPD com recursos adequados para fiscalização.
- Legislação e cooperação: apoiar a regulamentação da LGPD e promover parcerias nacionais e internacionais para segurança cibernética.

➢ Eixo de Transformação Digital "F. Transformação Digital da Economia":

- F1. Economia Baseada em Dados:
    - Criação de um ecossistema robusto para o desenvolvimento da economia de dados: inclui incentivos para o desenvolvimento de infraestruturas de telecomunicações e atração de *data centers* para o país. Essas infraestruturas são essenciais para a coleta, o armazenamento e o processamento de dados em larga escala, necessários para o funcionamento de cidades inteligentes.
    - Aprimoramento das capacidades técnicas e humanas em relação ao uso e tratamento de grandes volumes de dados: fundamental para garantir a segurança jurídica, a privacidade e o uso ético de dados em cidades inteligentes.
    - Promoção de um ambiente jurídico-regulatório que estimule investimentos e inovação: visa conferir segurança aos dados tratados e proteção adequada aos dados pessoais, essa ação é crucial para garantir a confiança digital e a segurança jurídica no contexto de cidades inteligentes.
    - Aprimoramento da política de dados abertos: envolve todos os entes federativos e a sociedade civil, incentivando a interoperabilidade e processos baseados em dados. A

política de dados abertos pode contribuir para a transparência e a participação cidadã na gestão de cidades inteligentes.

- F2. Um Mundo de Dispositivos Conectados:

  - Fomento ao desenvolvimento e à implantação de ambientes/plataformas para validação e avaliação de soluções de Internet das Coisas (IoT): especialmente para as áreas de Cidades 4.0. A criação desses ambientes controlados permite testar e aprimorar as soluções de IoT antes de sua implementação em larga escala em cidades inteligentes. O estímulo à IoT, com a devida governança sobre os dados tratado, é fundamental para o desenvolvimento sustentável das cidades inteligentes.
  - Promoção e fomento da escalabilidade e replicabilidade de plataformas abertas nacionais de IoT: direcionadas para os setores priorizados no plano de IoT, incluindo cidades inteligentes. A criação de plataformas abertas e escaláveis facilita a integração de diferentes soluções e a expansão dos serviços em cidades inteligentes.
  - Atualização do Marco Legal da Ciência, Tecnologia e Inovação[189]: visa aumentar a interação entre centros de pesquisa e empresas, e a articulação entre infraestruturas de pesquisa e linhas de fomento para o desenvolvimento de dispositivos conectados. A atualização do marco legal pode contribuir para a criação de um ambiente mais favorável à inovação em tecnologias para cidades inteligentes, incluindo a IoT.

- F3. Novos Modelos de Negócio:

  - Aprimoramento das condições competitivas entre plataformas *online* e intermediários: busca mitigar os efeitos de rede e de *lock-in* decorrentes da escala das plataformas digitais. Essa ação visa promover um ambiente de negócios mais equilibrado e competitivo, beneficiando o desenvolvimento de soluções inovadoras para cidades inteligentes.

[189] V. E-Digital, Ciclo 2022-2026, pág. 71. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosestrategiadigital/e-digital_ciclo_2022-2026.pdf

- Utilização de mecanismos de absorção, no setor público, de Tecnologias da Informação e Comunicação (TIC) desenvolvidas por *startups* e empresas. Essa medida pode impulsionar a inovação em tecnologias para cidades inteligentes, por meio da contratação de soluções desenvolvidas por *startups* e empresas.

Estratégia Nacional de Governo Digital[190]

15. A Estratégia Nacional de Governo Digital para o período de 2024 a 2027 tem como objetivo geral a busca de um Estado mais inclusivo, eficaz, proativo, participativo e sustentável[191].

16. Destacamos os seguintes objetivos e as respectivas recomendações que se relacionam com a transformação digital, especialmente no contexto das cidades inteligentes, e com a tutela da proteção de dados pessoais:

- Objetivo 4: Ampliar a resiliência e a maturidade tecnológica com foco em privacidade, proteção de dados e segurança cibernética
  - 4.1: Instituir governança para privacidade, proteção de dados pessoais e segurança cibernética.
  - 4.2: Criar planos de ação com controles e soluções tecnológicas para proteger dados pessoais.
  - 4.3: Designar encarregado pelo tratamento de dados pessoais e gestor de segurança da informação.
  - 4.4: Promover capacitação sobre privacidade, proteção de dados e segurança cibernética.

- Objetivo 5: Qualificar decisões e serviços com uso ético e interoperável de dados

[190] Está prevista na Lei nº 14.129, de 29 de março de 2021 (Lei do Governo Digital), mas foi formalizada pelo Decreto nº 12.069, de 21 de junho de 2024. A Portaria SGD/MGI nº 4.248, de 26 de junho de 2024 estabelece recomendações para o alcance dos objetivos para o período de 2024 a 2027. Disponível em: https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/estrategianacional

[191] Em especial por meio: I- da oferta de soluções que atendam às necessidades da sociedade e reconheçam as desigualdades sociais e as barreiras de acesso aos serviços públicos; II- da adaptação de seus processos às demandas atuais da sociedade, com inovação, uso adequado de tecnologias, reuso seguro de dados e melhor aplicação dos recursos públicos; e III- da transparência, do acesso à informação, da participação social na formulação de políticas públicas e da promoção do desenvolvimento sustentável.

5.1: Implementar programas de governança de dados para qualificação de políticas públicas.
5.2: Adotar mecanismos de interoperabilidade e compartilhamento seguro de dados entre entes federativos.
5.4: Estimular o uso ético de análise de dados na tomada de decisões e personalização de serviços

- Objetivo 6: Garantir infraestrutura moderna e integração entre entes federativos
  6.5: Definir estratégias de armazenamento de dados, com foco em segurança, soberania e eficiência.
- Objetivo 7: Fomentar inovação e uso de tecnologias emergentes
  7.4: Desenvolver casos de uso de inteligência artificial e outras tecnologias, com atenção aos cuidados éticos.
  7.6: Utilizar infraestrutura tecnológica que promova o uso seguro de dados públicos e estimule a inovação.

Plano Nacional de Internet das Coisas[192]

17. Visa implementar e desenvolver a Internet das Coisas (IoT) no Brasil, promovendo a livre concorrência e a circulação de dados com segurança[193]. Dentre as vantagens apresentadas para estimular o desenvolvimento das cidades inteligentes, algumas delas reproduzidas pela ANPD em seu Estudo, são mencionadas:

- Melhoria de vida e eficiência: Visa melhorar a qualidade de vida e promover eficiência nos serviços por meio da IoT. (Art. 3º, I);
- Projetos mobilizadores: Estabelece Plataformas de Inovação e Centros de Competência para apoiar cidades inteligentes. (Art. 6º).

[192] Instituído pelo Decreto nº 9.854 de 2019. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/internet-das-coisas
[193] Seus objetivos incluem melhorar a qualidade de vida, capacitar profissionais, aumentar a produtividade das empresas, fomentar parcerias público-privadas e integrar o Brasil no cenário internacional. A Câmara IoT monitora e avalia a implementação do plano, promove parcerias e apoia projetos mobilizadores para alcançar esses objetivos.

- Prioridade para cidades: Ambientes urbanos são prioritários para aplicação de soluções de IoT (Art. 4º). São considerados critérios de oferta, demanda e capacidade de desenvolvimento local. (Art. 4º, §1º).
- Câmara das Cidades 4.0:[194] Lançada em 2019, é um fórum coordenado pelo Ministério do Desenvolvimento Regional (MDR) e pelo Ministério da Ciência, Tecnologia e Inovações (MCTI). Ela reúne instituições públicas e privadas e visa integrar a gestão dos serviços urbanos para alcançar os objetivos das cidades inteligentes. Criou iniciativas[195] como:
  - Carta Brasileira para Cidades Inteligentes: define o conceito de "cidades inteligentes" no Brasil. Propõe uma agenda para a transformação digital das cidades brasileiras visando o desenvolvimento urbano sustentável.
  - Plataforma de Diagnóstico de Maturidade para Cidades Inteligentes e Sustentáveis: Realiza diagnósticos para ajudar gestores públicos a identificar as condições atuais das cidades. Propõe diretrizes para a elaboração de políticas nacionais e municipais para cidades inteligentes e sustentáveis.
  - Plataforma ReDUS: Apoia pessoas e organizações a atuarem em rede para construir um futuro mais sustentável para as cidades.
  - Cartilha de Emendas Parlamentares 2023: Documento participativo que reflete o trabalho do MCTI e suas vinculadas em projetos e políticas públicas.
  - Ambientes de Inovação: Inclui parques tecnológicos, incubadoras, distritos de inovação e espaços de *coworking*. Explora sinergias entre institutos de pesquisa, governo e iniciativa privada.

Guia *Sandbox* para Cidades Inteligentes: Oferece um passo a passo para a adoção de tecnologias e validação de soluções inovadoras em cidades inteligentes.

18. Estudo conduzido pelo BNDES (Banco Nacional de Desenvolvimento Econômico e Social), em 2018, sobre o Plano Nacional de IoT (Internet das Coisas), mostrou que até 2025 as cidades inteligentes poderiam adicionar à economia brasileira entre US$ 900 mil e US$ 1,7 bi, considerando somente a IoT.[196]Sobre o tema, Comitê

[194] Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/camara-cidades.
[195] Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/camara-cidades-programas_iniciativas/
[196] Disponível em: https://cbic.org.br/enic-a-importancia-das-cidades-inteligentes-para-a-sociedade/

Gestor[197], composto por integrantes do BNDES e do MCTIC (Ministério da Ciência, Tecnologia, Inovações e Comunicações), apresentou a seguinte frase-guia da aspiração do Brasil em Internet das Coisas:

> "Acelerar a implantação da Internet das Coisas como instrumento de desenvolvimento sustentável da sociedade brasileira aumenta a competitividade da economia, fortalece as cadeias produtivas nacionais, e promove a melhoria da qualidade de vida".

2.2. INICIATIVAS INTERNACIONAIS SOBRE CIDADES INTELIGENTES E O TRATAMENTO DE DADOS PESSOAIS

19. Internacionalmente, vale citar o Programa sobre Cidades Inteligentes e Crescimento Inclusivo[198] lançado pela OCDE em 2019. A iniciativa destaca o papel crucial da inteligência artificial (IA) e das tecnologias de aprendizado de máquina (ML) na realização de cidades inteligentes, contribuindo com soluções em diversas áreas do desenvolvimento urbano, como segurança, mobilidade e eficiência energética.

20. Nesse programa são destaques experiências estrangeiras na elaboração de políticas públicas direcionadas para o desenvolvimento de cidades inteligentes, como as dos países apresentados a seguir (OCDE, 2019):

> **1. Japão:** o governo japonês formulou a "Arquitetura de Referência para Cidades Inteligentes" (SCRA) para orientar o desenvolvimento de iniciativas de cidades inteligentes em todo o país e compartilhar a experiência acumulada de iniciativas existentes. O SCRA destaca a importância da interoperabilidade de plataformas de compartilhamento de dados para que outras cidades possam acessar e usar dados abertos disponíveis. O Japão também criou a Plataforma de Parceria Público-Privada para Cidades Inteligentes em 2019, visando acelerar as iniciativas de cidades inteligentes com empresas, universidades, instituições de pesquisa, autoridades locais e ministérios e agências relevantes como membros.
> **2. Coreia do Sul:** O governo coreano criou uma Estrutura de Governança de cidade inteligente por meio de Memorandos de Entendimento entre órgãos governamentais.

[197] Disponível em: https://www.bndes.gov.br/wps/wcm/connect/site/d1348f10-c93d-408e-8c2d-a2c2a6e4efb1/170614_Produto_Parcial_Frente+3_Aspiracao_IoT_Final.pdf?MOD=AJPERES&CVID=lOOiRj1
[198] Disponível em: https://www.oecd.org/en/about/programmes/the-oecd-programme-on-smart-cities-and-inclusive-growth0.html

3. Índia: O governo indiano desenvolveu a estratégia *"DataSmart Cities"* para ajudar a trabalhar a governança de dados de cidades inteligentes para resolver desafios urbanos complexos. A estratégia visa institucionalizar uma cultura de dados, estabelecendo mecanismos formais para coleta, gerenciamento e uso de dados.

21. Diversas outras iniciativas próprias de cidades inteligentes envolvendo evidências sobre a necessidade de tratamento de dados, inclusive pessoais, podem ser citadas mundo afora, conforme alguns exemplos trazidos no quadro abaixo (OCDE, 2023).

Cidades	Iniciativas
Viena, Áustria	A cidade implementou a "Estratégia de Excelência Digital" com o objetivo de dominar o ciclo de vida dos dados em todas as áreas da administração, minimizando o esforço e gerando o maior valor agregado possível por meio de dados.
Londres, Reino Unido	O bairro de Camden organizou uma consulta aos cidadãos, onde o governo forneceu diferentes cenários sobre como o bairro poderia usar os dados para melhorar os serviços públicos. O governo de Londres também criou o *London Datastore,* um portal gratuito e aberto de compartilhamento de dados.
Barcelona, Espanha	A cidade nomeou um *Chief Data Officer (CDO*) local para liderar as estratégias de dados e cidades inteligentes.
Bilbao, Espanha	O Conselho Municipal de Bilbao usa dados para criar novos serviços e melhorar os existentes, com base nos princípios do "Manifesto de Dados de Bilbao".
Takamatsu, Japão	A cidade desenvolveu a "Plataforma Comum de IoT da Cidade Inteligente" para gerenciar dados em áreas como gerenciamento de desastres, turismo e bem-estar.
Toyama, Japão	A cidade organiza o "Sketch Lab", um fórum para colaboração, cocriação e parcerias com empresas, universidades e outras partes interessadas.

22. Enfatizando os benefícios que as cidades inteligentes trazem para a sociedade e para o país, as cidades mais inteligentes do mundo chegam até a participar de uma competição internacional, o *World Smart City Awards,* que premia iniciativas inovadoras para cidades mais sustentáveis, habitáveis e economicamente viáveis. Em 2024, com 429 inscrições de 64 países venceu como cidade mais inteligente Shenzhen, na China. Em 40 anos, Shenzhen evoluiu de vila de pescadores a metrópole moderna, destacando-se por políticas e tecnologias inovadoras que impulsionaram governança, transporte, sustentabilidade, economia digital e qualidade de vida. Além dessa, a cidade de Espoo, na Finlândia, se destacou por sua estratégia de liderança de impacto, lançada

em 2019, que usa decisões baseadas em dados, projetos-piloto inovadores e treinamento para promover o desenvolvimento sustentável e enfrentar os desafios urbanos.[199]

23. O desenvolvimento tecnológico e a Internet das Coisas[200] são premissas básicas para o avanço das cidades inteligentes.

24. A OCDE estima que o mercado global de cidades inteligentes crescerá de USD 511,6 bilhões em 2022 para mais de USD 1.024 bilhões em 2027, com um CAGR (*Compound Annual Growth Rate* ou Taxa de Crescimento Anual Composta)[201] de quase 15% (em 5 anos). Em paralelo, o tamanho do mercado global de IA deve crescer de USD 177 bilhões em 2023 para cerca de USD 2,7 bilhões em 2033, com um CAGR de 37% entre 2024 e 2033, destacando a escalada e a importância econômica das tecnologias digitais nas configurações urbanas.

25. Existem ainda dois relatórios, elaborados pela OCDE, que destacam a importância das cidades inteligentes com uma abordagem mais particularizada e voltada para o ser humano, a saber:

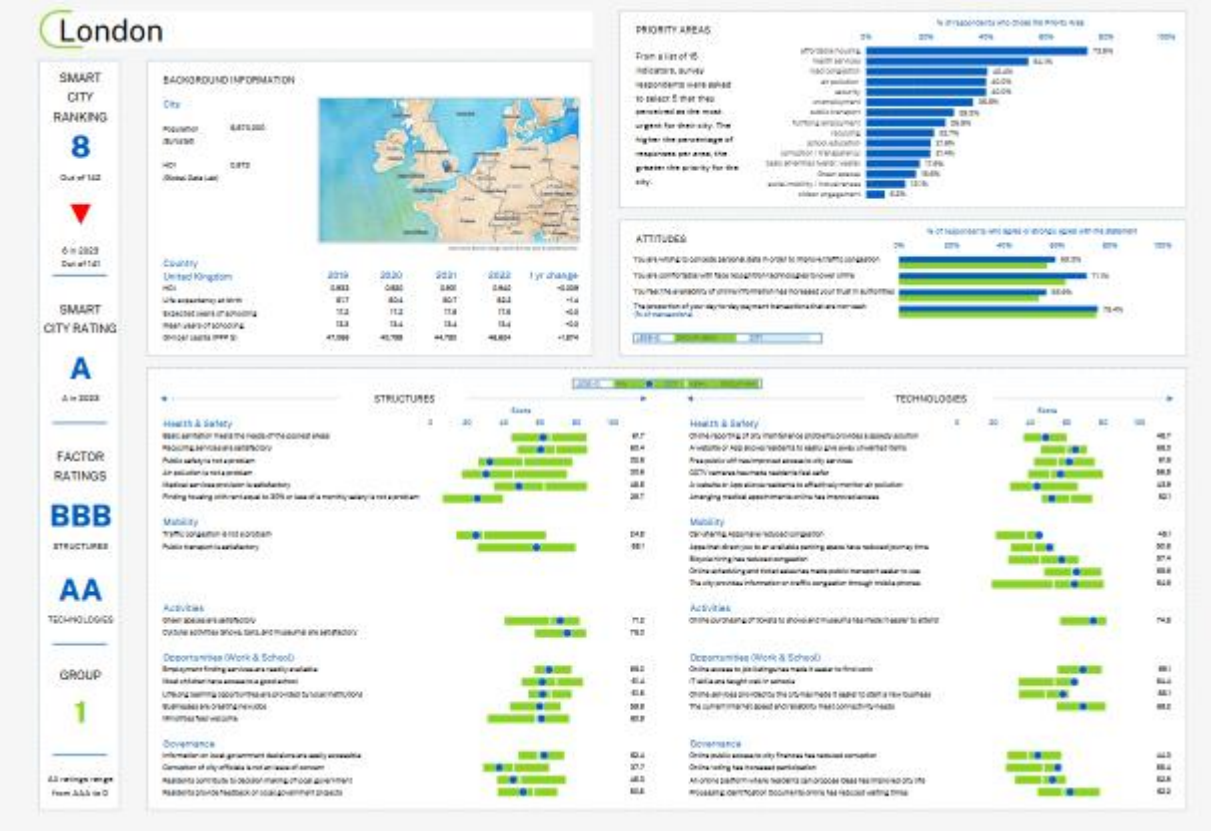
- "*Leveraging Digital Technology and Data for Human-centric Smart Cities: The Case of Smart Mobility* (2020)[202]: destaca a importância de alavancar a tecnologia digital e os dados para cidades inteligentes centradas no ser humano, com foco na mobilidade inteligente.
- "*Smart City Data Governance: Challenges and the Way Forward*[203]" (2020): examina os desafios e oportunidades relacionados à governança, segurança e interoperabilidade de dados em cidades

[199] Disponível em https://www.smartcityexpo.com/world-smart-city-awards-winners/
[200] Nesse contexto algumas tecnologias se destacam, como inteligência artificial (IA), deep learning (DL), aprendizado de máquina (machine learning, ML), Internet das Coisas (IoT), computação móvel, big data, blockchain, redes 6G, WiFi-7, Indústria 5.0, sistemas robóticos, sistemas de aquecimento/ ventilação/ar condicionado (HVAC), forense digital, sistemas de controle industrial, veículos conectados e automatizados (CAVs), veículos elétricos, reciclagem de produtos, carros voadores, backup de despensa (salvaguarda de alimentos), rede 6G (ANPD, 2024).
[201] Trata-se de uma métrica utilizada para calcular a taxa média de crescimento anual de um valor ao longo de um período específico, levando em conta o efeito dos juros compostos.
[202] Preparado pelo *International Transport Forum* (ITF) da OCDE e pelo Centro da OCDE para Empreendedorismo, PMEs, Regiões e Cidades, como uma contribuição para discussões no *G20 Digital Economy Task Force* em 2020, sob a Presidência da Arábia Saudita. https://www.itf-oecd.org/sites/default/files/docs/data-human-centric-cities-mobility-g20.pdf
[203] OECD (2023), Smart City Data Governance: Challenges and the Way Forward, OECD Urban Studies, OECD Publishing, Paris, https://doi.org/10.1787/e57ce301-en.

inteligentes. com uma abordagem centrada no ser humano enfatiza a necessidade de estruturas de governança eficazes para gerenciar o uso, armazenamento e compartilhamento de dados.

26. Outro *benchmark* internacional é o *Smart City Index* anual[204], produzido pelo IMD (*International Institute for Management Development),* que avalia cidades inteligentes com foco equilibrado em aspectos econômicos, tecnológicos e nas "dimensões humanas" como qualidade de vida, meio ambiente e inclusão. Nos últimos dois anos, em parceria com a *World Smart Sustainable Cities Organization* (WeGO), o índice coletou dados de 142 cidades desde 2019, tornando-se uma ferramenta importante para formuladores de políticas e atraindo a atenção internacional. Foram elaborados estudos de caso detalhados para mostrar os diferentes estágios de desenvolvimento das cidades inteligentes, abordando questões como o tratamento de dados pessoais. Um exemplo é Londres, que ficou em 8ª colocação (V. gráfico a seguir).

[204] Disponível em: https://www.imd.org/smart-city-observatory/home/rankings/



27. Todas essas iniciativas evidenciam a importância do tratamento de dados pessoais para o desenvolvimento das cidades inteligentes, cujo maior objetivo, numa compreensão ampla, é de proporcionar o a qualidade de vida do indivíduo, o bem-estar da coletividade e o desenvolvimento econômico e tecnológico do país.

3. CONFORMIDADE LEGAL E USO ÉTICO DOS DADOS PESSOAIS, NO BRASIL E EM OUTRAS JURISDIÇÕES

28. Como demonstrado, a eficácia dos projetos de cidades inteligentes depende significativamente da disponibilidade e uso de dados, inclusive pessoais. Algumas preocupações surgem quanto à conformidade legal e uso ético de tais dados, no que toca, especialmente à: (i) Vigilância e Controle; (ii) Uso comercial dos dados; (iii) Vazamento de dados; (iv) Usos secundários não esperados; (v) Compartilhamento de dados de maneira inadequada; (vi) Discriminação e aspectos éticos; (v) Perda da qualidade do dado. (ANPD, 2024).

29. Entretanto, visando compatibilizar o tratamento de dados pessoais e o desenvolvimento das cidades inteligentes, a ANPD sugere medidas mitigadoras de riscos aos indivíduos, demonstrando apoio ao tratamento de dados para esse fim ao considerar como medidas eficazes[205]:

1. Estabelecimento de políticas de privacidade robustas
   Implementar instituições, práticas e procedimentos que assegurem a prestação de contas e garantam recursos adequados para o gerenciamento, auditoria e acesso responsável aos dados pessoais.
2. Fortalecimento da segurança cibernética
   Priorizar a proteção digital ao implementar tecnologias nas cidades, adotando especificações técnicas rigorosas, criptografia de dados, monitoramento contínuo, controles de acesso e avaliações regulares de riscos.
3. Promoção da transparência
   Assegurar que indivíduos e comunidades sejam informados sobre a coleta e uso de seus dados pessoais, oferecendo-lhes a oportunidade de participar desse processo sempre que possível.
4. Processamento local de dados
   Sempre que viável, realizar o processamento de dados diretamente no dispositivo de coleta, transmitindo apenas informações analíticas ou agregadas para a rede ou nuvem, reduzindo o tráfego de dados pessoais.
5. Minimização na coleta de dados
   Coletar somente os dados essenciais para os fins previstos, mantendo-os armazenados apenas pelo período necessário para atender às finalidades definidas.
6. Supervisão de fornecedores e parceiros
   Selecionar e monitorar fornecedores e parceiros de forma rigorosa, garantindo auditorias regulares e inserindo cláusulas específicas de proteção de dados e segurança da informação nos contratos.
7. Integração da privacidade no design
8. Incorporar os princípios de proteção de dados desde as etapas iniciais do desenvolvimento de soluções *(privacy by design)*, garantindo a conformidade em todo o ciclo de vida do produto ou serviço.
9. Aplicação de técnicas de anonimização e pseudonimização

[205] Estudo Preliminar da ANPD sobre Cidades Inteligentes, 2024.

Utilizar métodos que reduzam ou eliminem a identificabilidade dos dados, tornando-os irreversíveis (anonimização) ou controlados de forma segura por meios reversíveis (pseudonimização).

10. Implementação de medidas contra discriminação
    Garantir que as soluções tecnológicas atendam às necessidades públicas, promovendo equidade e evitando impactos negativos sobre populações vulneráveis.

30. O já citado estudo conduzido pelo BNDES em parceria com o MCTIC sobre o Plano Nacional de IoT, finalizado em outubro de 2017[206], já abordava essa problemática de proteção de dados no contexto das cidades inteligentes. Ele traz uma Cartilha de Cidades[207] que busca oferecer recomendações para gestores públicos interessados em incorporar soluções de IoT e os principais pontos de atenção durante a implementação de soluções de IoT em cidades, com foco na privacidade, segurança da informação e armazenamento de dados pessoais.

31. Segundo a Cartilha, a coleta de dados deve equilibrar a eficiência das soluções tecnológicas com a proteção da privacidade dos cidadãos. Há uma distinção entre dados pessoais (que identificam indivíduos) e dados anonimizados, sendo os primeiros sujeitos à legislação específica. Recomenda-se anonimização, agregação e técnicas de *privacy by design* e de segurança da informação para mitigar riscos, bem como um cuidado com a base legal adequada e a observância estrita da finalidade para as quais os dados foram coletados.

32. Além disso, estudos revelam que a confiança da população assume um papel relevante de facilitador da estabilidade social, sendo considerada fundamental para um setor público se tornar "*data-driven*[208]. Uma vez confiando em seus governos, os cidadãos têm maior probabilidade de compartilhar dados para melhoraria de serviços públicos, por exemplo, ao passo que o uso inadequado ou sem permissão desses dados prejudica a confiança que pode levar anos para ser restaurada. (OCDE, 2023, p. 101).[209]

[206] Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/internet-das-coisas-estudo-repositorio

[207] Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinternetdascoisas/fase4_13_cartilha-de-cidades.pdf

[208] OECD (2019), The Path to Becoming a Data-Driven Public Sector, OECD Digital Government Studies, OECD Publishing, Paris, https://doi.org/10.1787/059814a7-en.

[209] OECD (2022[31]), Building Trust to Reinforce Democracy: Main Findings from the 2021 OECD Survey on Drivers of Trust in Public Institutions, https://doi.org/10.1787/b407f99c-en.

33. Nesse particular, a ANPD destaca, em seu Estudo, a "Confiança no Ambiente Digital" (eixo C, da Estratégia Brasileira de Transformação Digital), que visa garantir a confiança e a proteção dos direitos dos usuários, com ênfase no uso ético de tecnologias disruptivas, como a Internet das Coisas (IoT).

34. No Brasil, além da LGPD, que traz diretrizes sobre o tratamento de dados pessoais, inclusive no contexto de cidades inteligentes, o Código de Defesa do Consumidor, o Código Civil, o Marco Civil da Internet, a Lei de Acesso à informação precisam ser observados.

35. Em outras jurisdições, leis e regulamentam relevantes se destacam quando as cidades inteligentes envolvem tratamento de dados pessoais, como: Regulamento Geral de Proteção de Dados (GDPR), da UE [210]; Japão[211]: Ato de Proteção de Informações Pessoais (APPI) (2003, emendada em 2020); Coreia do Sul: Lei de Proteção de Informações Pessoais (2022)[212]; e Reino Unido: *Data Protection Act* (2018).

36. Além da legislação propriamente dita, inúmeros frameworks podem ser encontrados em normas da ISO/IEC. Como são diversos, apresentaremos apenas alguns exemplos elencados por tema:

- **Mobilidade inteligente e transporte:** são exemplos: **ISO 37157:2018** (Transporte inteligente para cidades compactas); **ISO 37158:2019** (Transporte inteligente usando ônibus movidos a bateria para serviços de passageiros); **ISO 37159:2019** (Transporte inteligente para trânsito rápido em áreas urbanas e arredores); **ISO 37180:2021** (Transporte inteligente com autenticação por QR Code em sistemas de transporte e serviços adicionais); **ISO 37184** (Mobilidade sustentável e transporte – Framework para serviços de transporte compatíveis com comunicação 5G);

[210] EU (2022), General Data Protection Regulation (GDPR) Compliance Guidelines, European Union, https://gdpr.eu/
[211] Government of Japan (2003[43]), Act on the Protection of Personal Information. Disponivel em: https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en; Government of Japan (2013[44]), Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure (Act No. 27 of 2013 as Amended), https://www.dataguidance.com/legal-research/act-use-numbers-identify-specific-individual; Government of Japan (2016[45]),
官民データ活用推進基本法 [Basic Act on the Advancement of Public and Private Sector Data Utilisation],, https://japan.kantei.go.jp/policy/it/data_basicact/data_basicact.html.
[212] Government of Korea (2022), 개인정보보호위원회 [Personal Information Protection Commission]. Disponível em:https://www.pipc.go.kr/eng/index.do

- Estrutura de desenvolvimento das cidades inteligentes: ISO 37155-1:2020 (Estrutura para integração e operação de infraestruturas comunitárias inteligentes – Parte 1: Recomendações para interações entre infraestruturas); ISO 37155-2:2021 (Estrutura para integração e operação de infraestruturas comunitárias inteligentes – Parte 2: Estratégia holística para desenvolvimento, operação e manutenção);
- Geração de energia: ISO 37160:2020 (Infraestruturas comunitárias inteligentes – Infraestruturas de energia elétrica – Métodos de medição e requisitos para operações de gerenciamento de plantas)
- Compartilhamento de informações: ISO 37156:2020 (Diretrizes para troca de dados e compartilhamento para comunidades inteligentes); ISO 37170:2022 (Framework de dados para governança de infraestruturas baseada em tecnologia digital em cidades inteligentes); ISO/TS 37172:2022 (*Framework* de integração de dados urbanos para planejamento de cidades inteligentes).
- Resiliência e redução de desastres: ISO/TR 63030:2022 (Redução de riscos de desastres – Resultados da pesquisa e análise).
- Indicadores para avaliação de cidades inteligentes: ISO 37122[213].

4. PRÁTICAS A SEREM IMPLEMENTADAS PARA MELHORAR A PROTEÇÃO DE DADOS E SEGURANÇA JURÍDICA EM CIDADES INTELIGENTES

37. Nessa mesma toada, a OCDE igualmente contribui com a apresentação de tendências para governança de dados em cidades inteligentes. Tanto governos nacionais quanto locais trabalham para estabelecer uma arquitetura de dados que reflita padrões de qualidade, permita interoperabilidade e facilite a colaboração entre os interessados para aumentar a eficiência na gestão de dados.

38. De maneira mais concreta, aOCDE apresenta um conjunto de recomendações com base nas experiências internacionais discutidas nas seções anteriores. O objetivo é auxiliar os governos locais na formulação e implementação de estratégias eficazes para o uso e governança de dados, com base em cinco pilares:

[213] Based on Kristiningrum, E. and H. Kusumo (2021[74]), "Indicators of Smart City using SNI ISO 37122:2019", https://doi.org/10.1088/1757-899X/1096/1/012013.

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

1. **Definição de Objetivos e Estratégias:** As cidades devem estabelecer uma visão clara sobre o papel dos dados no desenvolvimento urbano, definindo prioridades estratégicas e como os dados podem ajudar a atingir os Objetivos de Desenvolvimento Sustentável, criando estruturas de governança e promovendo a colaboração entre governos e setores.
2. **Gestão de Dados e Alfabetização Digital:** É importante adotar práticas de gestão de dados que garantam qualidade, confiabilidade e segurança, além de capacitar servidores públicos em habilidades digitais e promover a alfabetização digital entre os cidadãos.
3. **Proteção de Dados e Privacidade:** A proteção dos dados pessoais e a privacidade dos cidadãos são essenciais para gerar confiança. As cidades devem implementar medidas de segurança, garantir a conformidade com a legislação de proteção de dados e promover transparência no uso das informações.
4. **Interoperabilidade e Cooperação:** A interoperabilidade entre sistemas é crucial para o compartilhamento eficiente de dados. As cidades devem adotar padrões abertos, promover a colaboração entre diferentes órgãos e participar de iniciativas nacionais e internacionais.
5. **Co-criação e Participação das Partes Interessadas:** A participação cidadã e de outras partes interessadas é fundamental. As cidades devem criar mecanismos de consulta, envolver os cidadãos na definição de prioridades e promover a colaboração entre governo, setor privado e sociedade civil.

39. No pilar "*3. Priorização da Proteção de Dados e Privacidade e Transparência no Uso, Armazenamento e Compartilhamento de Dados*", destacamos as importantes recomendações para Governos Nacionais e Para Governos Locais propostas pela OCDE (2023, p. 176):

Recomendações da OCDE para Proteção de Dados em Cidades Inteligentes

Governos Nacionais	- Destacar a importância da proteção de dados no framework nacional de cidades inteligentes; - Promover políticas consistentes de privacidade de dados entre os governos subnacionais, bem como o desenvolvimento da força de trabalho em cibersegurança para harmonizar práticas entre os níveis de governo; - Definir e comunicar quaisquer obrigações de compartilhamento de dados dos governos subnacionais (por exemplo, para dados abertos);

	- Desenvolver uma estratégia de cibersegurança e plano de ação acompanhado de medidas para lidar com a escassez de força de trabalho em cibersegurança em coordenação com o setor privado e instituições de ensino;
Governos Locais	- Considerar as implicações éticas ao projetar estratégias de gestão de dados e cidades inteligentes para orientar comportamentos no setor público local, mitigar riscos e manter a confiança pública; - Adotar um código de conduta ou princípios éticos para a gestão de dados que promovam uma abordagem baseada em valores para dados e soluções de privacidade por design; - Verificar a integridade e adequação dos dados utilizados para promover responsabilidade e confiança; - Solicitar consentimento para coleta, armazenamento e uso de dados e fornecer mecanismos de exclusão; - Adotar uma abordagem multidisciplinar para lidar com questões de privacidade e segurança de dados, assegurando que o problema seja abordado por múltiplos ângulos políticos com apoio de diferentes partes interessadas; - Adotar uma abordagem de segurança por design em projetos de cidades inteligentes e conduzir análises de capacidades de cibersegurança para detectar lacunas de habilidades; - Comunicar abertamente aos cidadãos quais dados estão sendo coletados e com qual propósito; - Instalar uma equipe central para supervisionar os aspectos de segurança das tecnologias de cidades inteligentes com habilidades especializadas e responsabilidades além da administração de TI do dia a dia; - Garantir que qualquer coleta, processamento e publicação de dados sigam as regras de proteção de dados, minimizando o uso de informações pessoais e adotando mecanismos de auditoria para monitorar a adesão à especificação de propósito no processamento e retenção de dados.

40. Mencionado estudo da OCDE, de 2023, ainda traz exemplos de outros países e cidades específicas com descrição dos mecanismos que foram utilizados para ampliar o acesso a dados nas cidades inteligentes. Algumas medidas são nacionais, como o estímulo a dados abertos e interoperabilidade, como previsto na Estratégia Nacional de Dados do Japão, outros focam na esfera local, desenvolvendo uma política centrada no cidadão ao colocar as necessidades dos residentes no centro das políticas urbanas, como o exemplo de Barcelona, na Espanha. Outro exemplo é o de Londres: o governo da cidade criou o *London Datastore* como um banco de dados gratuito e aberto, no qual qualquer pessoa pode acessar cerca de 700 bases de dados relacionadas ao

progresso da cidade em questões como criação de empregos, transporte público, moradia, segurança comunitária etc.[214].

Abordagem	Local	Descrição
Estratégias Nacionais de Dados	Japão	- Promove dados abertos e interoperabilidade. - Utiliza tecnologias como IoT e IA para análise de dados. - Visa otimizar serviços públicos e inovação em cidades inteligentes.
	Reino Unido	- Enfatiza uso seguro e ético dos dados. - Estabelece diretrizes para proteção de dados pessoais. - Desenvolve frameworks para interoperabilidade de sistemas em cidades inteligentes.
Frameworks Padrões para Cidades Inteligentes	Índia	- Desenvolve uma ontologia unificadora para manejo de dados de diversas fontes. - Estabelece o Data Exchange Platform para lidar com dados em diferentes setores.
	Reino Unido	- Implementa o padrão PD 8100 para cidades inteligentes. - Foca em uniformizar abordagens de dados entre diferentes setores urbanos.
Abordagens Centradas no Humano no Uso de Dados	Viena (Áustria)	- Adota uma política centrada no cidadão, colocando as necessidades dos residentes no centro das políticas urbanas. - Utiliza dados para melhorar a acessibilidade e a personalização dos serviços urbanos.
	Paris (França)	- Foca em políticas de dados que promovem a reutilização de dados abertos. - Prioriza transparência e acesso público aos dados para estimular inovação e engajamento cívico.
Oficiais de Dados Locais para Liderança Estratégica	Barcelona (Espanha); Paris (França); Reykjavík (Islândia)	- Nomearam chefes de dados locais (oficiais municipais) para liderar e coordenar a estratégia de dados da cidade. - Focam em melhorar a governança de dados e a eficiência dos serviços públicos.

[214] Disponível em: https://data.london.gov.uk/

Abordagem	Local	Descrição
Estratégias Locais de Dados	Viena (Áustria); Londres (Reino Unido)	- Viena aborda silos de dados e responsabilidade incerta. - Londres usa dados para definir e atingir resultados políticos desejados.
Acesso e Reutilização de Dados Estruturados	Paris (França)	- Torna todos os dados estruturados acessíveis por meio de licenças abertas para promover sua reutilização e gerar novas aplicações.
Dashboards de Dados	Seul (Coreia do Sul)	- Desenvolveu dashboards que centralizam e visualizam dados urbanos de diferentes setores para produzir indicadores em tempo real, melhorando a tomada de decisões e a transparência.

5. CONCLUSÃO

41. Para o desenvolvimento sustentável das cidades inteligentes, com sua inerente complexidade e interseção de tecnologias avançadas, é fundamental a adoção de uma abordagem ética, responsável e segura no tratamento de dados pessoais e o cumprimento rigoroso da legislação de proteção de dados é imprescindível para assegurar os direitos e liberdades dos titulares, garantindo segurança jurídica.

42. O estudo em questão destaca a importância da transparência no tratamento de dados pessoais dos residentes dessas cidades, pois permite avaliar as ações do governo e ainda estabelece uma relação de confiança entre os indivíduos e as autoridades. Além disso, o estudo traz exemplos de iniciativas que mitigam riscos com o objetivo de criar estruturas de governança robustas, assegurando a segurança das informações pessoais, como a (i) promoção de políticas públicas centradas no indivíduo; (ii) o estímulo à interoperabilidade entre sistemas; (iii) a abertura de dados para acesso amplo da população, bem como a articulação entre os entes públicos e a colaboração destes e dos diversos setores e residentes. Ao conciliar inovação tecnológica com a observância dos princípios éticos e legais no tratamento de dados pessoais, é possível construir cidades mais inclusivas, eficientes e sustentáveis, promovendo o bem-estar coletivo sem comprometer os direitos de liberdade dos indivíduos. Diante da magnitude do tema e da relevância das cidades inteligentes para o país, é de importância fundamental sua abordagem e incentivo na PNPD.

São Paulo, 16 de dezembro de 2024.

Rony Vainzof
Conselheiro Titular do CNPD.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANEXO XXV – ESTUDO DE CASO: CRIANÇAS E ADOLESCENTES

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ESTUDO DE CASO: CRIANÇAS E ADOLESCENTES

por Isabella Henriques

Introdução[215]

O direito à proteção de dados pessoais e à privacidade é garantido às crianças e aos adolescentes, assim como a todas as pessoas naturais. No caso desse grupo social, contudo, existe a necessidade de uma abordagem diferenciada, haja vista toda a gama de direitos humanos que lhes são consagrados, seu melhor interesse e o peculiar estágio de desenvolvimento no qual se encontram.

Dados pessoais estão na esfera dos direitos da personalidade e o seu uso indiscriminado pode objetificar as pessoas, afetar o desenvolvimento da sua personalidade, promover manipulações e gerar discriminações ilegais. Por isso, quando tais riscos são transpostos para a esfera infantojuvenil, deve-se também considerar a proteção jurídica especial que assiste crianças e adolescentes.

Vale dizer que crianças e adolescentes muitas vezes sequer possuem os recursos necessários para a devida compreensão da complexidade das discussões relacionadas à proteção de dados pessoais, à privacidade e à sociedade da informação/ conhecimento, quanto menos dos abusos passíveis de serem perpetrados, especialmente no ambiente digital. Se é desafiador a uma pessoa adulta com um bom nível de instrução, mais ainda para a criança e o adolescente.

Mesmo quando foi alfabetizada, a criança não compreende, por exemplo, longos termos de uso e políticas de privacidade de plataformas, aplicativos e dispositivos digitais, hermeticamente escritos, com linguagem formal e técnica. Crianças e adolescentes são menos conscientes dos modelos, das consequências e das ameaças do tratamento de seus dados pessoais. Daí, podem acabar tendo seus dados pessoais tratados sem que tenham o devido conhecimento ou dimensão do impacto disso em suas vidas.

[215] Introdução com trechos retirados do capítulo Regulação normativa do ambiente digital no Brasil das Múltiplas Infâncias; Lei Geral de Proteção de Dados (LGPD); O art. 14 da LGPD de Isabella Henriques no livro Direitos fundamentais da criança no ambiente digital. São Paulo: Thomson Reuters, Revista dos Tribunais, 2023.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

Por nascerem imersos em um mundo dominado pelas tecnologias digitais, crianças e adolescentes possuem, comparativamente aos adultos, uma perspectiva de muito mais tempo de tratamento de seus dados pessoais, ao longo de suas vidas, gerando os chamados 'rastros digitais', por um período muito maior e com reflexos mais duradouros. Todos esses fatores fazem com que haja uma exigência ainda maior em relação à proteção dos seus dados pessoais e privacidade.

Não que crianças e, principalmente adolescentes, não tenham certa capacitação de manuseio das novas tecnologias digitais da informação e comunicação. Contudo, muitas vezes, não conseguem compreender as complexas dinâmicas de causa e consequência atreladas a essas ferramentas. Com isso, não usufruem plenamente os recursos disponíveis, com conhecimento e repertório necessários.

Dessa forma, mesmo que crianças e adolescentes constituam conhecimento no sentido de se apropriarem das novas tecnologias digitais da informação e da comunicação, ainda assim – em especial as crianças mais novas – são hipervulneráveis diante do contexto vigente de hiperexposição de dados pessoais, especialmente, no ambiente digital. Isso porque, o desenvolvimento humano cognitivo e psicossocial é um processo complexo que está atrelado a diversos fatores, inclusive etários, culturais e socioeconômicos. Trata-se de uma construção paulatina, que exige tempo e vivências, em um entrelaçamento entre a constituição genética e o ambiente no qual se está inserido. É por tudo isso que "crianças e adolescentes compõem o grupo mais vulnerável de pessoas cujos dados pessoais circulam na ubiquidade dos meios informáticos"[216].

1. Práticas Nacionais e Internacionais:

Importa mencionar, de partida, que as normas internacionais acerca da proteção de dados pessoais e da centralidade do ser humano no ambiente digital devem ser aplicáveis a crianças e adolescentes. A Resolução do Conselho de Direitos Humanos das Nações Unidas, de 2013, 'Direito à privacidade na era digital', originada de projeto então apresentado pelo Brasil juntamente com a Alemanha, dentre outros Estados[217], reafirma o direito à privacidade, tal qual previsto na Declaração Universal de Direitos Humanos e no Pacto Internacional de Direitos Civis e Políticos, bem como convoca os países a respeitarem e protegerem o direito à privacidade

[216] HENRIQUES, Isabella; PITA, Marina; HARTUNG, Pedro. A proteção de dados pessoais de crianças e adolescentes. *In* MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; e RODRIGUES JR., Otavio Luiz (coord.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021, p. 201.
[217] UNITED NATIONS. General Assembly adopts 68 resolutions, 7 decisions as it takes action on reports of its third committee. A/C.3/68/L.45/Rev.1. 2013. Disponível em: https://www.un.org/press/en/2013/ga11475.doc.htm (Acesso em: 9 Dez 2024)

de seus cidadãos. E recomenda sejam providas medidas efetivas de reparação a violações e que qualquer restrição ao direito à privacidade respeite os princípios da necessidade, legalidade e proporcionalidade, pareando, ainda, o alcance dos direitos humanos na realidade física com a virtual. Nesse sentido, todos os direitos humanos, inclusive aqueles consagrados pela Convenção sobre os direitos da criança da ONU, são válidos também no ambiente digital[218] [219]: *"the same rights that people have offline must also be protected online"* [220]. Devem ser respeitados, protegidos e cumpridos nesse espaço, de forma que as crianças e os adolescentes, nas suas múltiplas infâncias e adolescências, tenham garantidos seus direitos de maneira efetiva em todos os espaços que percorrem.

- Comentário Geral nº 25 sobre os direitos das crianças em relação ao ambiente digital do Comitê dos Direitos da Criança (ONU)

O Comentário Geral nº 25 (CG25) [221], elaborado pelo Comitê dos direitos da criança da ONU, é o documento mais completo e de alcance global sobre o tema dos direitos humanos de crianças e adolescentes no ambiente digital e também sobre as peculiaridades do tratamento de seus dados pessoais e da privacidade nessa esfera. Expressamente, garante o direito supranacional à proteção especial estabelecido pela Convenção sobre os direitos da criança da ONU também no ambiente digital. Afirma o dever de proteção reforçada e de devida diligência para a proteção integral das crianças, no sentido de que os países signatários da Convenção previnam e evitem violações também por parte dos agentes não estatais, por meio de iniciativas legislativas, administrativas e políticas, bem como pela fiscalização e por medidas de reparação.

[218] NETMUNDIAL. NETmundial multistakeholder statement Global multistakeholder Meeting on the future of Internet governance, 2014. Disponível em https://netmundial.br/2014/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf (Acesso em: 9 Dez 2024).

[219] UNITED NATIONS HUMAN RIGHTS OFFICE OF THE HIGH COMMISSIONER. OHCHR and privacy in the digital age. Disponível em: https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx (Acesso em: 9 Dez 2024).

[220] HUMAN RIGHTS COUNCIL OF UNITED NATIONS. The promotion, protection and enjoyment of human rights on the Internet. United Nations, 2021. Disponível em: https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx (Acesso em: 9 Dez 2024).

[221] COMMITTEE ON THE RIGHTS OF THE CHILD OF UNITED NATIONS. General comment n. 25 on children's rights in relation to the digital environment. Convention on the rights of the child. Genebra: United Nations, 2021. Disponível em: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation (Acesso em 9 Dez 2024).

Possui quatro princípios estruturantes: não-discriminação; melhor interesse da criança; direito à vida, à sobrevivência e ao desenvolvimento; e respeito pela opinião da criança. Entre as inovações recomendadas está a sugestão de criação de um "órgão governamental encarregado de coordenar políticas, diretrizes e programas relacionados aos direitos das crianças entre os departamentos do governo central e os vários níveis de governo" e que haja monitoramento independente das políticas públicas. Em relação ao setor empresarial é contundente ao incluí-lo como parte responsável por garantir os direitos da criança e do adolescente, prevendo a necessidade de que as empresas realizem avaliações de impacto dos direitos dessas pessoas no ambiente digital. Recomenda, ainda, sejam proibidos o perfilamento e a publicidade direcionada a crianças e adolescentes, para fins comerciais "com base em um registro digital de suas características reais ou inferidas, incluindo dados grupais ou coletivos, publicidade direcionada por associação ou perfis de afinidade". Da mesma forma, também recomenda a proibição de práticas dependentes de "*neuromarketing*, análise emocional, publicidade imersiva e publicidade em ambientes de realidade virtual e aumentada para promover produtos, aplicações e serviços". (citações em traduções livres)

Sobre o direito à privacidade assevera ser "vital para a agência, dignidade e segurança das crianças e para o exercício de seus direitos". Menciona que as ameaças à privacidade de crianças e adolescentes podem surgir da coleta e processamento de dados por instituições públicas, empresas e outras organizações. Diz que, ainda que sejam rotineiras práticas digitais como processamento automatizado de dados, perfilamento, direcionamento comportamental, vigilância em massa, entre outros, é certo que podem violar o direito de crianças e adolescentes à sua privacidade e "podem ter consequências adversas sobre as crianças, que podem continuar a afetá-las em estágios posteriores de suas vidas". Por isso assevera que deve ser observado o princípio da minimização de seus dados, de forma que a coleta e o processamento sejam proporcionais e limitados. O CG25 diz que a regulação sobre o tema deve ser feita por legislação e "por *design* em produtos e serviços digitais que afetam crianças". Eventual consentimento para a coleta e processamento de dados de crianças e adolescentes, segundo o CG25, deve ser antecipado, informado e dado livremente por eles ou, a depender de sua idade, por sua mãe, pai ou responsável. Dados coletados devem ser facilmente acessados pelas crianças ou adolescentes, por suas mães, seus pais ou responsáveis, bem como passíveis de retificação quando for necessário ou de apagamento quando armazenados ilegal ou desnecessariamente. Indica a necessidade de serem realizadas auditorias regulares e medidas de prestação de contas por aqueles que coletarem e processarem dados de crianças e adolescentes. Também menciona que deve ser permitido o uso de avatares *online* ou pseudônimos que protejam a identidade das crianças e dos adolescentes. Essas pessoas também devem ser protegidas da vigilância digital. O CG25 encoraja os países a introduzir ou atualizar a regulação de proteção de dados e padrões de *design*, que de alguma forma interfiram no direito de crianças e

adolescentes – em especial quando interfiram na liberdade do pensamento e crença no ambiente digital, por meio, por exemplo, de análise emocional, inferência ou manipulação.

- Manifesto para uma melhor governança de dados de crianças (UNICEF)

O documento 'The case for better governance of children's data: A manifesto – What does a better model of data governance for children look like?' lançado pelo UNICEF, em 2021[222], segue sendo uma referência na temática. É um documento que traz a conhecimento alguns problemas relativos ao tratamento de dados de crianças e adolescentes, apontando lacunas específicas nas políticas e práticas em relação ao tema. Estabelece parâmetros aspiracionais para encorajar governos e o setor privado a finalmente endereçar os direitos de crianças e adolescentes em atuais e futuras estruturas de governança de dados. O documento defende um tratamento diferenciado para os dados de crianças e adolescentes, sob o fundamento de serem mais vulneráveis em relação aos adultos e menos capazes de compreender as implicações de longo prazo relacionadas ao tratamento de seus dados. Também porquanto as consequências da vigilância e do rastreamento são mais significativas para crianças e adolescentes, no presente e no futuro, devido à maior exposição ao longo de suas vidas, assim como por serem a infância e a adolescência períodos de desenvolvimento e experimentação. A partir dessas premissas, o Manifesto apresenta dez ações para articular uma melhor abordagem quanto aos dados de crianças e adolescentes, a serem consideradas pela comunidade global, por ocasião do desenvolvimento e implementação de estruturas de governança de dados:

1. Proteger crianças e seus direitos por meio de uma governança de dados centrada na criança. Essa governança de dados deve aderir aos acordos internacionais no sentido de minimizar o uso de vigilância e algoritmos de perfilamento do comportamento de crianças.
2. Priorizar os melhores interesses da criança em todas as decisões sobre seus dados.
3. Considerar a identidade única de cada criança, capacidades e circunstâncias em evolução nas estruturas de governança de dados. É necessário haver certa flexibilidade para dar conta da criança em processo de desenvolvimento, além de contemplar também crianças marginalizadas.

[222] UNITED NATIONS CHILDREN'S FUND (UNICEF). The case for better governance of childrens data: A manifesto – What does a better model of data governance for children look like?. Nova Iorque: Unicef, 2021. Disponível em: https://www.unicef.org/innocenti/media/1036/file/UNICEF%20Global%20Insight%20Data%20Governance%20Summary.pdf (Acesso em: 9 Dez 2024).

4. Alterar a responsabilidade pela proteção de dados das crianças para empresasa e governos. As medidas de proteção devem ser estendidas para todos abaixo de 18 anos, independente da idade de consentimento.
5. Colaborar com crianças e suas comunidades na construção de políticas e gestão de seus dados. Em outras palavras, empoderar crianças e suas comunidades para ditar como e por quem os dados serão processados, e com quem podem ser compartilhados.
6. Representar o interesse das crianças dentro de processos administrativos e judiciais, bem como mecanismos de reparação.
7. Providenciar recursos adequados para implementar estruturas de governança de dados que sejam inclusivos com crianças. As autoridades de proteção de dados e empresas de tecnologia precisam empregar pessoal que entenda sobre o direito de crianças e adolescentes, e governos precisam alocar fundos para fiscalização.
8. Usar políticas de inovação em governança de dados para solucionar problemas complexos e acelerar resultados para crianças.
9. Preencher lacunas de conhecimento na governança de dados de crianças e adolescentes. É preciso assegurar, por meio de pesquisas, que as regulamentações de governança sejam baseadas em evidência.
10. Fortalecer a colaboração internacional para governança de dados de crianças e promover transferência de conhecimento e políticas entre países. A falta de coordenação em nível nacional pode levar a competição entre jurisdições e conflitos, e por isso o Manifesto encerra com esse direcionamento.

Nessa toada, relevante mencionar a importância dos conceitos de *'privacy by design'* – no sentido de que a privacidade seja pensada em todo o ciclo do tratamento, desde o desenvolvimento do produto ou serviço – e *'privacy by default'* – para que as regras mais protetivas de privacidade sejam aplicadas como padrão, sem a exigência de ações das pessoas usuárias para tanto. No caso de crianças e adolescentes também cabe dizer *'children's rights by design'* como um padrão no tratamento de dados de crianças e adolescentes[223].

- União Europeia

[223] HARTUNG, Pedro. The children's rights-by-design standard for data use by tech companies. Unicef, 2020. Disponível em: https://www.unicef.org/innocenti/reports/childrens-rights-design-standard-data-use-tech-companies (Acesso em: 9 Dez 2024).

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

(i) Verificação etária na União Europeia

Em fevereiro de 2023, o Serviço de Pesquisas do Parlamento Europeu apresentou uma relação quanto às formas de verificação etária no ambiente digital utilizadas na União Europeia, tecendo alguns comentários sobre cada uma, no sentido de se robustecer esse que é um tópico relevante para a proteção especial de dados e privacidade de crianças e adolescentes[224]:

- Autodeclaração: mais comum das formas de verificação e facilmente contornada por crianças;
- Cartão de crédito: pessoas usuárias precisam comprovar a validade de um cartão de crédito, fazendo um pagamento de valor irrisório (como um centavo). Método mais utilizado por usuários de sites que vendem produtos para o público adulto (bebidas alcoólicas ou pornografia, por exemplo). Há risco de "*phishing*" e é muito possível que alguém use um cartão que não é seu.
- Biometria: método utilizado a partir de tecnologias de Inteligência Artificial e tecnologias biométricas, como o reconhecimento facial, conforme regulamentado pela União Europeia[225]. A IA seria capaz de analisar as feições e determinar a idade. Suscetível de erros; a pessoa pode usar a imagem de uma pessoa mais velha; métodos biométricos estão associados a problemas de privacidade por serem calcados em categorias especiais de dados pessoais. Risco de tratamento excessivo de dados e perfilamento.
- Análise dos padrões de uso online: método de verificação por inferência, por meio, por exemplo, da importação do histórico de navegação da pessoa usuária, da aplicação de questionários ou da análise do conteúdo gerado pelo usuário ou por compras feitas. Há também grandes riscos de privacidade envolvidos.
- Verificação offline: feitas por meio de documentos de forma situacional.

[224] European Parliament. Online age verification methods for children. Disponível em: https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739350/EPRS_ATA(2023)739350_EN.pdf (Acesso em: 9 Dez 2024)
[225] European Parliament. Regulating facial recognition in the EU. European Parliamentary Research Service, Setembro 2021. Disponível em: https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739350/EPRS_ATA(2023)739350_EN.pdf (Acesso em: 9 Dez 2024).

- **Consentimento de mães e pais**: alguns serviços e aplicações exigem consentimento parental para registrar crianças e adolescentes em determinados serviços digitais. Contudo, a autoridade parental raramente é verificada, o quê seria feito idealmente por meio da conferência de documentos de identidade ou registros familiares.

- **"Vouching"**: envolve perguntar a pessoas que não são as mães ou os pais para atestar de forma online sobre a idade do usuário envolvido.

- **Identidade Digital**: método que se apoia nas ferramentas oferecidas por determinado país para verificar a identidade e idade do usuário antes de garantir acesso a serviços digitais. China, Canadá e Austrália já introduziram a identidade digital, e a própria União Europeia criou sua carteira de identidade digital (abordada na sequência).

- **Verificação etária por aplicativo específico**: é o caso da França, em que há necessidade de instalar um aplicativo de certificação digital, licenciado pelo governo, para acessar conteúdo pornográfico na Internet.

Esse é um tópico bastante relevante para a proteção dos dados e privacidade de crianças e adolescentes, pouco tratado e carente de inovação no Brasil. As evoluções no tema implementadas por empresas em diferentes partes do globo, como por regulações de outros países não devem ser transpostas para a realidade nacional sem as devidas análises e adaptações, mas podem informar o processo de tomada de decisão por agentes privados e autoridades públicas nacionais.

(ii) A carteira de identidade digital da União Europeia

Solução desenvolvida para autenticar a identidade das pessoas, viabilizar o acesso dos usuários a serviços online, guardar e compartilhar documentos digitais, e criar assinaturas vinculantes. A ideia da União Europeia[226] é que todo membro da UE ofereça seu próprio aplicativo da Carteira para cidadãos, residentes e negócios nos próximos anos — mas todos são desenvolvidos de acordo com as mesmas especificações. Cada versão da Carteira será interoperável e funcionará em qualquer lugar da Europa.

A funcionalidade de guardar da Carteira permite o armazenamento e compartilhamento de vários documentos, desde carteiras de motorista até cartões de academia, por exemplo. Essa ferramenta é

[226] The Wallet. What are EU Digital Identity. Disponível em: https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/What+is+the+wallet (Acesso em: 9 Dez 2024).

interessante no contexto de crianças e adolescentes, para permitir acesso rápido e digital a documentos relacionados à parentalidade ou responsabilidade legal.

A União Europeia também dedicou uma página para as especificações técnicas da Carteira.

(iii) Verificação etária e soluções tecnológicas

Há investimentos significativos, no contexto da União Europeia, para desenvolver novas soluções tecnológicas para o problema da verificação etária.

No dia 15 de outubro de 2024, a Comissão Europeia divulgou um concurso público ("*call for tenders*") para o desenvolvimento, consultoria e suporte para uma solução em relação ao tema de verificação etária[227]. A iniciativa é calcada no dever de proteção de crianças e adolescentes, uma das prioridades nos termos do Digital Services Act (DSA) e da implementação da estratégia Better Internet for Kids (BIK+).

Nos termos do DSA, todas as plataformas digitais precisam assegurar um alto nível de segurança e privacidade para crianças e adolescentes. Ainda de acordo com esse diploma, são estabelecidas obrigações específicas para plataformas de larga escala e ferramentas de busca de larga escala. Referidas plataformas possuem o dever de mitigar riscos, por exemplo, aplicando uma política robusta de verificação da idade para todos os usuários, quando apropriado.

Há também um dever, estabelecido pela Declaração Louvain-la-Neuve de integrar ferramentas do DSA com a Carteira de Identidade Digital Europeia, a fim de assegurar proteções robustas para os usuários de serviços digitais na União Europeia — especialmente grupos vulneráveis.

O concurso contou com um orçamento de 4 milhões de euros. Seu objetivo foi desenvolver especificações técnicas, com *input* dos estados membros e outros stakeholders, para uma solução de verificação etária que preserve a privacidade. Ou seja, promover soluções para a verificação das pessoas usuárias sobre se possuem mais de 18 anos sem compartilhar nenhuma outra informação sobre a pessoa.

[227] European Commission. Shaping Europe's digital future. Call for tenders: Development, consultancy and support for na age verification solution. European Union: Outubro, 2024. Disponível em: https://digital-strategy.ec.europa.eu/en/funding/call-tenders-development-consultancy-and-support-age-verification-solution (Acesso em: 9 Dez 2024).

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

A ideia é criar uma aplicação genérica (white label) para ser publicada pelos estados membros nas lojas de aplicativos, com base no Zero-Knowledge Proof protocol (um recurso que permite verificar se um atributo é verdadeiro sem revelar quaisquer outros detalhes).

- Brasil

Em relação à proteção de dados de crianças e adolescentes, o país possui um único artigo específico na LGPD, que é o art. 14. Ainda que seja insuficiente para dar conta de todos os desafios, o fato de apresentar o termo "melhor interesse" tem o condão de ensejar a efetividade dos direitos fundamentais desse grupo social. De toda a forma, a sua aplicação tem se mostrado um enorme desafio, que impõe a necessidade de uma série de medidas por todas as partes envolvidas: poder público, sistema de justiça, empresas, sociedade, famílias e as próprias crianças e adolescentes. Exemplos disso são os casos em face de Meta e Tiktok em trâmite na ANPD, que intenta dar efetividade para o "melhor interesse" na proteção de dados e privacidade de crianças e adolescentes.

Nesse sentido, o "melhor interesse" exige que o tratamento de dados de crianças e adolescentes seja feito, também no Brasil, com as diligências necessárias, também acompanhado da elaboração e publicização de relatórios de avaliação de risco e de impacto, com base na Resolução nº 245/24 do Conanda, Convenção sobre os direitos da criança da ONU, CG25, Constituição Federal, Estatuto da Criança e do Adolescente e LGPD, de maneira que haja proteção integral e prioritária desse grupo de pessoas hipervulnerável, a fim de reforçar o dever de sua proteção e cuidado, também por parte da iniciativa privada, tal qual indicado pelo Instituto Alana, em 2022, na sua contribuição para a tomada de subsídios da ANPD sobre o tratamento de dados pessoais de crianças e adolescentes: 'O melhor interesse de crianças e adolescentes e as bases legais aplicáveis ao tratamento de seus dados pessoais'.

2. Conformidade legal e uso ético, no Brasil e em outras Jurisdições:

O CG25 indica que os Estados nacionais devem implementar políticas públicas por meio de "regulações, códigos industriais, padrões de design e planos de ação em conformidade, todos os quais devem ser regularmente avaliados e atualizados" (tradução livre) que tenham como objetivo proporcionar às crianças e aos adolescentes a oportunidade de beneficiarem-se de seu envolvimento com o ambiente digital e assegurar seu acesso seguro. Menciona que crianças em situação de desvantagem ou vulnerabilidade devem receber apoio às suas necessidades, com informações acessíveis, até traduzidas para idiomas minoritários relevantes. A LGPD estabelece princípios relevantes, como a boa fé, o acesso à informação, a não discriminação, a

transparência, a prevenção de danos, a responsabilização e a prestação de contas, bem como fomenta a existência de códigos de ética para as empresas promoverem o cumprimento da lei.

Algumas boas medidas podem ser vislumbradas em propostas legislativas em tramitação ou já aprovadas (mas ainda não em vigor) nos EUA e no Age Appropriate Code do Reino Unido: auditoria independente para plataformas de mídia social, no sentido de avaliarem os riscos e os impactos a crianças e adolescentes, bem como a conformidade com a legislação; ampliação de transparência para a sociedade em relação a dados críticos das plataformas de mídias sociais; fornecimento às famílias de um canal para relatarem danos a crianças e adolescentes; desabilitação de recursos online considerados viciantes; e a garantia de opções pelo não recebimento de recomendações algorítmicas. Também a promoção de um *design* de salvaguardas para a proteção de dados em produtos e serviços online, para que se garanta sejam apropriados ao uso de crianças e adolescentes, atendendo às suas necessidades, como, por exemplo, configurações padrão com minimização de coleta e uso de dados e com o recebimento de orientações e conselhos, inclusive sobre o uso dos dados dessas pessoas (Age Appropriate Design Code UK).

Também é uma boa prática a existência e funcionamento de uma área regular de *compliance* de dados, que não seja meramente de fachada, tais como código de conduta, de ética e de políticas, controles, investigações e procedimentos internos, formações, canais de denúncia, *due diligence*, relatórios de análise de riscos e envolvimento da liderança.[228] No contexto em que a proteção de dados é fator ético intrínseco aos modelos de negócio baseados em IA, o *compliance* de dados pessoais de crianças é também parte essencial para o uso ético de sistemas e aplicações de IA. Fundamental, assim, que a heterroregulação incentive não só a conformidade por meio de sistemas de *compliance*, mas também o adequado desenvolvimento de tecnologias éticas "para o fim de evitar o deter- minismo tecnológico desenhado e imposto pelos agentes econômicos mais poderosos"[229].

[228] HENRIQUES, Isabella. O papel dos mecanismos de compliance e das políticas de proteção de dados para a proteção de dados pessoais de crianças e adolescentes. CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (coordenadores). Compliance e políticas de proteção de dados. São Paulo: Revista dos Tribunais, 2021, pp. 369-398.
[229] FRAZÃO, Ana. Propósitos, desafios e parâmetros gerais dos programas de *compliance* e das políticas de proteção de dados. CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (coordenadores). Compliance e políticas de proteção de dados. São Paulo: Revista dos Tribunais, 2021, p. 50.

Exemplo de código a ser utilizado, também, como incentivo ao *compliance* de dados de crianças é o holandês 'Code voor kinderrechten' ou, em inglês, 'Code for children's rights'[230]. Lançado em março de 2021, foi elaborado pela Universidade de Leiden e pela organização Waag Technology & Society, a pedido do Ministério do Interior e de Relações do Reino. Já foi utilizado em ações judiciais envolvendo empresas, na qualidade de instrumento de interpretação da legislação. Ainda que tenha tido declarada inspiração no britânico Age Appropriate Design Code e tenha sido endossado pela 'Autoridade Holandesa para Consumidores e Mercados' não constitui legislação oficial. Ou seja, não é mandatório, mas as leis nas quais se baseia são.

No caso brasileiro vale mencionar, ainda sobre o tema, a contribuição do Instituto Alana para a Consulta Pública da ANPD sobre a norma de Aplicação da LGPD para agentes de tratamento de pequeno porte, intitulada 'A prioridade absoluta da proteção dos dados pessoais de crianças e adolescentes pela ANPD e por agentes de tratamento de pequeno porte' (2021).

3. Meios para aumentar a proteção de dados e segurança jurídica:

É fundamental que sejam evitados incidentes de segurança envolvendo dados de crianças e adolescentes. Como exemplo, vale rememorar o incidente de segurança da empresa CloudPets, fabricante de bichos de pelúcia conectados à Internet, que deixou públicos cerca de 2 milhões de gravações de voz de mães, pais, responsáveis e crianças, além de 800 mil dados de cadastro de seus clientes, em fevereiro de 2017[231]. Incidente semelhante aconteceu em 2014, quando a central de armazenamento da fabricante de dispositivos digitais voltados a crianças, VTech foi hackeada e os dados de 5 milhões de indivíduos foram expostos, inclusive, selfies de crianças[232], motivando o FTC a multar a empresa em 2018, pela coleta de dados de crianças sem

[230] DIGITAL FUTURES COMMISSION. The Dutch approach to realise children's rights in a digital world: Code voor kinderrechten. 5Rights Foundation, 2022. Disponível em: https://digitalfuturescommission.org.uk/blog/the-dutch-approach-to-realise-childrens-rights-in-a-digital-world-code-voor-kinderrechten/ (Acesso em: 9 Dez 2024).
[231] FRANCESCHI-BICCHIERAI, Lorenzo. Internet of Things teddy bear leaked 2 million parent and kids message recordings. Motherboard – Tech by Vice, 2017. Disponível em: https://www.vice.com/en/article/internet-of-things-teddy-bear-leaked-2-million-parent-and-kids-message-recordings/ (Acesso em: 9 Dez 2024).
[232] BARRETT, Brian. Hack brief: Hacker strikes kids' gadget maker VTech to steal 5 million accounts. Wired, 2015. Disponível em: https://www.wired.com/2015/11/vtech-childrens-gadget-maker-hack-5-million-accounts// (Acesso em: 9 Dez 2024).

autorização prévia dos responsáveis legais e por falhar ao tomar medidas preventivas de segurança da informação.

Também essencial que dados de crianças e adolescentes não sejam tratados simplesmente por estarem em meio a dados de adultos sem que sejam tomadas as providências necessárias para que isso não ocorra.

Finalmente, entre as boas práticas possíveis estão as medidas de verificação etária, procedimentos como auditorias, elaboração de relatórios de avaliação de risco e de relatórios de avaliação de impacto quanto ao tratamento de dados de crianças e adolescentes, mais transparência e meios de comunicação efetivos com a sociedade, as famílias e as próprias crianças e adolescentes, dentre tudo o que foi anteriormente abordado. Sempre, em consonância com a legislação e o dever de garantia da absoluta prioridade de crianças e adolescentes.

*****

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANEXO XXVI – ESTUDO DE CASO: ACESSO AO PODER PÚBLICO

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

Estudo de Caso

Acesso das esferas municipais, estaduais e federais a dados de interesse público

Conselheiro: Alexandre Boava
dezembro/2024

Esse estudo de caso tem como objetivo abordar o inciso "V" do Artigo 2º da LGPD, que consiste na proteção de dados pessoais a partir de um de seus fundamentos, o desenvolvimento econômico, tecnológico e inovação aplicado ao acesso das esferas municipais, estaduais e federais a dados de interesse público.

1. Dados produzidos em espaços públicos são de interesse público

O argumento de que os dados produzidos em espaços públicos são de interesse público baseia-se no entendimento de que tais informações podem contribuir significativamente para o desenvolvimento de políticas públicas, a promoção da transparência e o controle social, além de serem produzidos em espaços que contam com infraestrutura pública.

Primeiramente, dados gerados em espaços públicos, como fluxos de tráfego, localização de equipamentos públicos, registros ambientais, prestação de serviço e trabalho, têm potencial para beneficiar diretamente a coletividade. Essas informações ajudam na alocação de recursos, no planejamento urbano e em respostas rápidas a emergências sociais, além de fortalecer a garantia de todos o direitos fundamentais e humanos de cada cidadão. A disponibilização desses dados fomenta o desenvolvimento de soluções inovadoras, como aplicativos de transporte público, análise de segurança urbana e outras iniciativas tecnológicas que fortalecem o bem-estar coletivo.

Esse dados gerados em espaços públicos, contam invariavelmente com as infraestruturas existentes em cada território, ou seja, cidades e estados. Ruas, rodovias, calçadas, energia elétrica, internet, saneamento básico, são alguns exemplos de infraestruturas necessárias para que qualquer empreendimento produza dados. Empresas (controladores de dados) que produzem dados através de aplicativos de mobilidade, entrega, carona, saúde, educação, ou qualquer outra aplicação que produza dados no espaço público, só foi possível por conta da infraestrutura e condições econômicas da população do território.

Além disso, no Brasil, a Lei de Acesso à Informação (LAI) e princípios constitucionais reforçam o direito de acesso a dados de interesse público em caso de contratos públicos e sob ordem judicial e regulatória, desde

que respeitados limites como a privacidade e a segurança. Dados anonimizados e tratados de forma responsável podem ser amplamente utilizados sem infringir direitos individuais, atendendo ao equilíbrio entre transparência e proteção de dados, conforme a LGPD.

2. Aspectos éticos e legais: uso responsável dos dados e adequação à LGPD

Apesar dos benefícios que a utilização desses dados apresenta, é fundamental assegurar a conformidade com as legislações vigentes. Dados pessoais devem ser anonimizados, e o compartilhamento deve ocorrer dentro de uma estrutura legal clara, respeitando a privacidade dos usuários. A Lei Geral de Proteção de Dados (LGPD) no Brasil estabelece diretrizes claras para o tratamento de dados pessoais, mesmo quando coletados em espaços públicos. Para assegurar sua utilização legítima, os seguintes princípios devem ser observados:

1. **Finalidade e proporcionalidade:** Os dados devem ser usados exclusivamente para fins de interesse público e de forma proporcional ao objetivo definido.

2. **Transparência e prestação de contas:** A sociedade deve ser informada sobre quais dados estão sendo coletados, por quem e para que finalidade.

3. **Anonimização e segurança:** Sempre que possível, os dados devem ser anonimizados para proteger a privacidade individual e garantir sua segurança contra acessos não autorizados.

4. **Consentimento e exceções legais:** Quando aplicável, o consentimento deve ser obtido, exceto em casos previstos em lei, como execução de políticas públicas ou proteção da vida e segurança.

Ainda, a utilização desses dados exige responsabilidade por parte do poder público. Os dados se referem a pessoas reais e um tratamento inadequado pode expor e colocar em risco esses cidadãos. É necessário reforçar também que essas informações são utilizadas para subsidiar políticas públicas que igualmente refletem na vida dos titulares de dados. Ações mal feitas construídas a partir de análises meramente numéricas nesses casos podem levar ao crescimento do trânsito e até a acidentes fatais, por exemplo.

Nessa linha, Reis e Direito (2023) argumentam que meros algoritmos não podem suplantar agendas e decisões no ciclo da política pública. Tomadas de decisões via ciência de dados não podem ser caixas pretas, em que possíveis vieses (ou a ausência deles) criam mais desigualdades, por exemplo, em busca de um ótimo fiscal. São excelentes ferramentas que devem ser debatidas, ampliadas, monitoradas e fiscalizadas, mas

precisam de análises precisas e humanizadas, considerando o reflexo na vida das pessoas. O parâmetro deve passar pela avaliação de quais dados devem ser acessados e por que atores de forma a beneficiar a oferta e adequação de políticas públicas.

3. Tráfego viário no poder público: dados como recurso estratégico e responsabilidade social

Serviços de mapa e de navegação por GPS, como o Google Maps e o Waze, têm mudado a forma como governos e cidadãos entendem e gerenciam o tráfego viário. Com o avanço das tecnologias e a ampliação do acesso a smartphones e à internet, a capacidade dessas ferramentas de fornecer informações em tempo real sobre fluxo de veículos, congestionamentos e alternativas de rota representa um recurso valioso para a sociedade. O massivo volume de dados gerados por cada um dos milhões de usuários dessas plataformas espalhados pelas cidades traz informações precisas sobre tendências de tráfego, possibilita o desenho de trajetos mais rápidos, mapeia rotas de transporte público, permite a identificação de acidentes, bloqueios na pista e outras intempéries possíveis nas ruas, além de muitas outras potencialidades.

Esses gigantes bancos de dados carregam um valor imensurável para o poder público e o subsídio de políticas públicas diversas. Nas mãos dos gestores de trânsito, esses dados, se utilizados correta e responsavelmente, permitem o planejamento mais eficiente de intervenções, a redução de gargalos, o aprimoramento do transporte público, o aumento da segurança viária e um leque de oportunidades de diferentes áreas.

Pensando nesse potencial, essas empresas já possuem iniciativas e projetos voltados para a gestão pública em suas operações. O programa Waze for Cities (WFC), por exemplo, permite que o Waze e agências governamentais do mundo todo compartilhem dados para ajudar o planejamento da cidade, tomar decisões melhores sobre a infraestrutura e aumentar a eficiência das operações diárias. Em contrapartida, esses mesmos dados alimentam o banco das empresas e ajudam a melhorar as ferramentas com informações mais precisas e atualizadas desses locais. A Google Mobility Reports foi outra iniciativa que visava mensurar a eficácia das medidas de isolamento social durante a pandemia.

Vários municípios e estados brasileiros já utilizam essas tecnologias para operacionalização do trânsito, seja por meio de parcerias com essas empresas ou pelo simples uso das ferramentas disponibilizadas. O Governo do Rio Grande do Sul já disponibiliza através do Google Maps um mapa interativo que mostra

bloqueios em tempo real nas rodovias do Estado[233]. A ferramenta foi especialmente útil durante os alagamentos provocados por chuvas intensas. A Prefeitura do Rio de Janeiro opera um projeto em conjunto com a Google que visa a utilização de IA para controle dos semáforos de forma mais eficiente e que reduza pontos de tráfego e o tempo de espera dos motoristas[234].

4. Dados de tráfego como recurso de interesse público

Informações sobre tráfego são, sem dúvida, dados de interesse público. Eles impactam diretamente a qualidade de vida dos cidadãos, influenciam decisões econômicas e contribuem para a sustentabilidade ambiental ao promover soluções que reduzam emissões de poluentes. O uso desses dados por parte do poder público fortalece a tomada de decisões baseadas em evidências e viabiliza políticas mais eficazes para mitigar problemas como engarrafamentos crônicos e acidentes.

É essencial apontar que o uso desses dados pelo poder público é essencialmente diferente da utilização por parte das empresas que o produzem. O Estado utiliza esses dados para subsidiar a construção de políticas que beneficiem toda a população sem nenhum tipo de fim lucrativo, enquanto as empresas têm interesse primariamente comercial e visam viabilizar seus diferentes modelos de negócios, que vai além da própria oferta de serviços e passa pelo marketing e o tráfego pago, a criação de plataformas digitais, entre outros.

Ainda, a propriedade exclusiva desses dados por parte de empresas produzidos de forma predatória torna o poder público refém dos serviços fornecidos, sem poder recorrer a alternativas. As parcerias construídas de forma alguma devem manter exclusividade sobre os dados gerados no espaço público das cidades, dados estes de interesse público (Morozov; Bria, 2019). Os dados coletados são de interesse público e devem ser mantidos também pelo poder público de forma independente, sem afetar os direitos das empresas de tratá-los de forma comercial e nem necessariamente abri-los em definitivo para domínio público, com vistas a preservar sigilos comerciais e principalmente proteger os dados da população.

233 Disponível em <https://www.estado.rs.gov.br/governo-disponibiliza-mapa-interativo-que-mostra-bloqueios-em-rodovias-do-rs-em-tempo-real> Acesso em 07 dez 2024

234 Disponível em <https://www.tnh1.com.br/noticia/nid/entenda-como-funciona-o-projeto-do-google-que-testa-ia-em-semaforos-no-rio/>. Acesso em 07 dez 2024.

A publicação de dados produzidos por essas plataformas, como exemplificado por iniciativas municipais e estaduais, amplia o senso de responsabilidade e o engajamento cívico, possibilitando o monitoramento e a fiscalização das ações governamentais. A abertura desses dados para a gestão pública não é apenas uma ferramenta de gestão, mas também um instrumento para o exercício pleno da cidadania e do controle social. Portanto, enquanto respeita-se a privacidade e a segurança, o uso de dados públicos permite transformar informações dispersas em soluções que atendem às necessidades coletivas e fortalecem as bases de um governo mais transparente e responsivo às demandas sociais.

5. Experiências internacionais: transparência e democratização dos dados

Para complementar o debate, é interessante trazer algumas experiências internacionais, como os casos de Barcelona e do Reino Unido. A começar com a cidade catalã, que construiu com o acúmulo de anos de debate sobre o tema o projeto DECODE (Decentralised Citizen Owned Data Ecosystem, em português, Ecossistema de Dados Descentralizado de Posse dos Cidadãos). O projeto visa o desenvolvimento de tecnologias descentralizadas, como criptografia e blockchain, para promover ao povo maior acesso a dados.

Barcelona considera os dados como parte de sua infraestrutura, assim como energia elétrica e água, e possui um trabalho intenso de envolvimento da população com o debate, com políticas que consolidam normas de privacidade e proteção ao mesmo tempo em que disponibilizam essa infraestrutura a empreendimentos, centros de pesquisa e demais pessoas interessadas a fim de gerar valor para o espaço comum. Assim, a cidade adota uma abordagem baseada em normas internacionais e melhores práticas para assegurar que os dados sejam acessíveis, precisos e atualizados, promovendo a reutilização por cidadãos, empresas e pesquisadores para gerar inovação e melhorar serviços públicos.

Outra experiência internacional interessante trata dos conceitos e ferramentas por trás do open Contract Data Standard (OCDS), em português, Padrão de Dados de Contratação Aberta. O OCDS é um formato de contratação pública que permite a divulgação de dados e documentos em todas as etapas do processo de contratação, definindo um modelo de dados comum. Foi criado para ajudar organizações a aumentar a transparência nas contratações e possibilitar análises mais aprofundadas dos dados contratuais por uma ampla gama de usuários.

É um ótimo padrão para contratos públicos com empresas Software as a Service (SaaS) e afins, como seria o caso de parcerias com o Waze e Google Maps, pois permite não só a transparência no processo de contratação como também com a utilização de dados de interesse público. É o modelo utilizado na cidade de Barcelona, referência mundial em políticas urbanas de dados.

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

O Open Contract Data Standard em Barcelona faz parte das iniciativas de transparência e governança digital da cidade. Ele está vinculado ao movimento de dados abertos promovido pelo portal Open Data BCN, que visa maximizar a reutilização de informações públicas para promover transparência, inovação e desenvolvimento social e econômico.

Outra experiência que enriquece o debate é o caso da fundação Nesta no Reino Unido, uma fundação que atua pela democratização de dados de saúde. O conceito de "Health Knowledge Commons" defendido pela Nesta propõe um sistema de conhecimento aberto e colaborativo na área da saúde. Ele busca integrar diferentes fontes de informação — incluindo dados médicos, experiências de pacientes e pesquisas científicas — para criar uma base comum de conhecimento acessível a profissionais de saúde, pacientes e formuladores de políticas públicas.

Essa abordagem visa melhorar a tomada de decisões em tempo real, garantindo que todos os atores envolvidos tenham acesso às melhores evidências disponíveis. Elementos essenciais para essa visão incluem redes de comunicação entre pacientes e profissionais de saúde, uso de tecnologias de inteligência artificial para análise de dados e mudança cultural em relação à gestão da saúde individual e comunitária.

A criação desse tipo de sistema depende de colaboração intersetorial, políticas públicas voltadas para o compartilhamento responsável de dados e investimentos em infraestrutura digital e formação de competências. A iniciativa também destaca o papel de redes peer-to-peer e plataformas abertas como mecanismos para engajar cidadãos e profissionais de forma participativa.

Referências Bibliográficas

Ajuntament de Barcelona. (n.d.). *Technology accessible to everyone: Accessible and participatory*. Recuperado em 13 de dezembro de 2024, de https://ajuntament.barcelona.cat/digital/en/technology-accessible-everyone/accessible-and-participatory/accessible-and-participatory-6

Ajuntament de Barcelona. (n.d.). *Decode: Accessible and participatory*. Recuperado em 13 de dezembro de 2024, de https://ajuntament.barcelona.cat/digital/en/technology-accessible-everyone/accessible-and-participatory/decode

Google. (n.d.). *Waze for cities partners: How Waze helps cities*. Recuperado em 13 de dezembro de 2024, de https://support.google.com/waze/partners/answer/10618477?hl=pt-BR

Morozov, E., Bria, F. (2019). A cidade inteligente: tecnologias urbanas e democracia. São Paulo: Ubu Editora.

Nesta. (n.d.). *Creating a health knowledge commons*. Recuperado em 13 de dezembro de 2024, de https://www.nesta.org.uk/press-release/creating-a-health-knowledge-commons/

Open Contracting Partnership. (n.d.). *Open Contracting Data Standard*. Recuperado em 13 de dezembro de 2024, de https://standard.open-contracting.org/latest/en/

Reis, Fernanda Teixeira, & Direito, Denise do Carmo. (2023). Dados pessoais e políticas públicas: O que revelar e o que preservar? Revista Brasileira de Avaliação, 12(1), e121623. https://doi.org/10.4322/rbaval202312016

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANEXO XXVII – ESTUDO DE CASO: EFICIÊNCIA ENERGÉTICA E SUSTENTABILIDADE

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

Ao

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

GT5 do CNPD

Dados pessoais para o desenvolvimento econômico, tecnológico e a inovação Estudo de caso
11 - Eficiência energética e sustentabilidade

O setor de energia é estratégico para o desenvolvimento social e econômico da sociedade. Mais do que isso, é caminho da prosperidade para pessoas físicas e jurídicas.

Não por outra razão, tem sua guarda constitucional no que diz respeito às formulações e caminhos dos recursos energéticos, com competência privativa da União.

Nesse particular, criou, dentro contexto de manutenção e equilíbrio das relações que perfazem o setor de energia, agências reguladoras que, em nome do estado na sua configuração maior, atua na regulação, na fiscalização e controle das atividades de interesse público.

Com esse prisma estratégico é que a sustentabilidade do setor energético deve ser pauta mandatória nas agendas dos 3 poderes da república, em alinhamento com a política energética determinada pela União no seu papel constitucional de garantir a soberania e segurança energética ao nosso país.

Ganha relevo, portanto, as medidas necessárias para que a sociedade garanta a sustentabilidade energética.

Nesse particular, mais do que inovação, importa aprofundarmos os contornos da eficiência energética, ferramenta tão determinante ao alcance da sustentabilidade da energia desejada.

E com esse enfoque, dado que o setor de energia, nos últimos anos, ganhou contornos dinâmicos com maior participação do consumidor como ator ativo na geração de energia no sistema elétrico (papel até então tutelado, em absoluto, pelo estado brasileiro através da União), com o expressivo crescimento da energia solar, o crescimento relevante da eletrificação veicular, a adoção do armazenamento de energia, dentre outros novas tecnologias que estão determinando nova configuração no sistema elétrico e energético brasileiro.

Algumas ferramentas já foram implementadas pelo Brasil na busca de ampliar a eficiência energética pela sociedade, como, por exemplo, a boa política do Procel, selo conferido a equipamentos elétricos que sinalizam ao consumidor o seu nível de eficiência.

Outras formas surgiram, como a criação das bandeiras tarifárias (verde, amarela e vermelha), cujo objetivo é sinalizar ao consumidor de energia se o custo da geração de energia está mais alto ou mais baixo, a depender das condições climáticas, sistêmicas ou operacionais.

Não podemos deixar de fora também as acertadas medidas de fomento realizadas com os recursos de Pesquisa e Desenvolvimento e para aplicação de eficiência energética, que, anualmente, aplicam recursos financeiros através de uma fração da tarifa de energia em projetos devidamente habilitados que gerem inovações e novas aplicações ou, ainda, medidas de eficiência energética para um número relevante de consumidores.

Vale destacar no campo da eficiência energética algumas ações realizadas pelas distribuidoras de energia elétrica do país com vários atores da sociedade, como as medidas de substituição de lâmpadas em residências e também no parque de iluminação pública, troca de geladeiras e aparelhos industriais ou domésticos, que proporcionam uma redução do consumo de energia importante para a solidez e sustentabilidade do serviço de energia elétrica.

Mas não é só. Essa necessidade é cada vez maior e desafiadora, pois cada vez mais o mundo está eletrificado e cada vez menos tem-se recursos energéticos em condições equilibradas. E num cenário de intensa participação e interação do consumidor, na ponta do consumo ou na ponta da geração, é mandatório tomar outras medidas que garantam a sustentabilidade do serviço de energia em medida necessária aos consumidores e usuários.

É exatamente por isso, nesse mercado energético mais dinâmico, volátil e livre, é que medidas de sustentabilidade precisam ser mais presentes, transparentes e ativas.

É daí que surge, portanto, a necessidade de uma maior cautela com os dados energéticos (consumo, uso e geração) que influenciam na operação desse sistema de magnitude continental, como é o exato caso brasileiro, uma vez que, como sabemos, dispomos de um sistema elétrico interligado que uma medida no norte do país, afeta, por exemplo, a região sul, e vice versa.

Se ampliarmos, ainda mais desafiador, com as potencialidades de geração industrial, a transformação energética no mercado petrolífero, a eletromobilidade veicular, e outros vetores que influenciam essa balança energética nacional.

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

É preciso, portanto, cuidar, medir e adotar medidas alinhadas, não só com os interesses individuais desse consumidor protagonista ou ativo, mas também, e principalmente, da coletividade, do todo, da nação, com enfoque absoluto na sustentabilidade.

E nessa abordagem é também preciso incluir os dados da realidade, como IDH, PIB, Renda Familiar, CENSO, Cadastro único e outros indicadores sociais econômicos que atestam a complexidade geográfica e social do País, tão igual em conceito frio, mas tão diferentes na sua realidade.

E com essa visão, precisamos encontrar ângulos, fórmulas e orientadores que ganhem relevância nessa gestão da sustentabilidade e eficiência energética.

Entendo que as razões desses indicadores, seus motivadores e finalidades, se melhor estudados com essa ótica da sustentabilidade, podem contribuir para a formulação de novas prescrições no sentido de garantir condições mais equilibradas para o desenvolvimento econômico, tecnológico e inovação no setor de energia.

É de se estimar que algumas práticas possam ser implementadas para a obtenção desse aprimoramento das políticas públicas em torno da sustentabilidade do setor de energia em meio a essa atual, crescente e acelerada transformação tecnológica e sistêmica:

i. Maior grau de informações de uso, consumo e geração por parte dos formuladores (poder concedente) e asseguradores das políticas públicas e serviços concedidos (agências reguladoras, órgãos e empresas vinculadas e que detenham papéis de organização, manutenção e formulação setorial);

ii. Maior integração e cruzamento desses dados para que se busque leituras mais adequadas na busca da desejada sustentabilidade e eficiência energética;

iii. Estabelecer diretrizes complementares aos agentes setoriais no sentido de fornecer determinadas informações dos consumidores e usuários para que seja viável o estudo e estabelecimento de medidas mais objetivas por questões sócio econômicas e geográficas;

iv. Elaborar diretrizes conjuntas (ministérios e agências) para que se estabeleçam responsabilidades e papéis na construção dessa base de dados capaz de melhor permitir a leitura de cenários, achados e outros elementos, que contribuirão para tomada de medidas tendentes à crescente sustentabilidade dos recursos energéticos nacionais à sociedade.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANEXO XXVIII – ESTUDO DE CASO: MARKETING E PUBLICIDADE

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ESTUDO DE CASO

TRATAMENTO DE DADOS PESSOAIS PARA FINS DE MARKETING E PUBLICIDADE[235]

1 - Introdução:

O crescente avanço tecnológico e a transformação digital têm destacado a relevância dos dados pessoais como um ativo estratégico para o desenvolvimento econômico, tecnológico e a inovação. Ao mesmo tempo, a proteção desses dados e o uso responsável das informações pessoais são desafios centrais para governos, empresas e a sociedade em geral. Nesse contexto, a formulação de políticas públicas adequadas é crucial para equilibrar a promoção da inovação com a garantia dos direitos fundamentais à privacidade e à proteção de dados.

O presente estudo tem como objetivo subsidiar as atividades do Grupo de Trabalho 5 (GT5), criado pela Portaria CNPD nº 05, de 4 de outubro de 2024 dedicado a fornecer subsídios, na temática de dados pessoais para o desenvolvimento econômico, tecnológico e a inovação, para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade, por meio da análise das práticas de tratamento de dados pessoais no âmbito do marketing e da publicidade, especialmente no que tange a publicidade personalizada e a criação de perfis comportamentais.

Desta forma, apresentaremos práticas nacionais e internacionais para análise das atividades de tratamento e proteção de dados para fins de marketing no Brasil e no exterior, tanto pelas Autoridades de Proteção de Dados como modelos de Autorregulação publicitária, com o objetivo de mapear o impacto da proteção de dados no desenvolvimento econômico, tecnológico e na inovação responsável.

Com essa abordagem, o estudo pretende oferecer contribuições para a formulação de uma Política Nacional de Proteção de Dados que permita às práticas de marketing evoluir de forma ética e inovadora, assegurando o equilíbrio entre desenvolvimento econômico, avanço tecnológico e a proteção de direitos fundamentais.

[235] Documento Elaborado por Vitor Morais de Andrade, com a colaboração de Lygia Maria Moreno Molina e Amanda Lenz Bender

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

A conformidade legal, aliada à transparência e à adoção de práticas éticas, é essencial não apenas para atender às exigências regulatórias, mas também para fortalecer a confiança dos indivíduos nas empresas e organizações, e criar um ecossistema sustentável, responsável e competitivo.

2 - Publicidade personalizada por meio da criação de perfil comportamental

O uso de dados pessoais para marketing e publicidade é uma prática amplamente difundida e essencial para empresas de diversos setores econômicos. A seguir, serão exploradas em maior profundidade as práticas de marketing e publicidade relacionadas à criação de perfis comportamentais.

O *profiling* é uma prática que permite, através do uso da tecnologia, a criação perfis de consumidores a fim de prever comportamentos e direcionar ofertas e serviços com maior precisão. Consiste, portanto, na criação de perfil de um indivíduo, com base em diversas informações, as quais podem incluir preferências de navegação, hábitos de consumo, interações em mídias sociais, informações sobre dispositivos utilizados e informações fornecidas pelo próprio usuário.

A partir da formação de perfil, as empresas têm como objetivo, comumente, conhecer o usuário e suas preferências e, a partir daí, inferir seus interesses e exibir publicidade, produtos ou serviços personalizados, que tenham relevância ao usuário. Ao utilizar esta prática para oferta de produtos e serviços, as empresas podem personalizar suas ações de marketing com base no comportamento e preferências dos consumidores e, por consequência, têm como benefícios atingir públicos específicos e interessados com a maior probabilidade de conversão e redução do desperdício de recursos financeiros de todos envolvidos. De outro lado, o consumidor recebe ofertas alinhadas aos seus interesses e necessidades e, possivelmente, tem uma redução da exposição à publicidade indesejada e conteúdos que sejam irrelevantes para ele. Ainda, tem seus esforços de buscas reduzidos e maior economia de tempo, tendo em vista a otimização de sua experiência de compra.

Recentemente, a McKinsey divulgou dados que mostram que empresas que investem na publicidade personalizada têm aumento das receitas entre 5 e 15%, e incremento do ROI (retorno sobre investimento) de 10 a 30%. Do ponto de vista dos consumidores, 71% esperam que as empresas ofereçam interações

personalizadas e, ainda, 76% se frustram quando isso não acontece[236]. Ainda, em estudo divulgado em 2023 pela PwC, 47% dos entrevistados no Brasil responderam que estariam dispostos a pagar 10% a mais por produtos feitos sob medida ou personalizados e, além disso, 45% utilizam assinaturas de serviços em razão da possibilidade de personalização[237].

Considerando este cenário, o presente estudo abordará, a seguir, legislações, práticas e estratégias que orientam o tratamento de dados pessoais para fins de marketing e publicidade, tanto no contexto nacional quanto internacional, respeitando os direitos e garantias dos titulares, ao mesmo tempo em que se preservam as atividades do setor empresarial.

3 - Conformidade legal e uso ético: práticas de conformidade para publicidade personalizada por meio da criação de perfil comportamental.

Esta seção tem como objetivo explorar práticas de conformidade e governança ética em diversas jurisdições, com ênfase no papel de marcos regulatórios, destacando como essas normas promovem o uso responsável de dados pessoais em marketing e publicidade personalizada.

3.1. Brasil:

A Lei Geral de Proteção de Dados – LPGD (Lei nº 13.709/2018)[238] define dado pessoal como "*informação relacionada à pessoa natural identificada ou identificável*" (art. 5º I). Apesar de não conceituar "identificável", entende-se que, sempre que informações combinadas permitirem a identificação de um titular, consideram-se dados pessoais, nos termos da Lei[239].

---

[236] Disponível em https://www.mckinsey.com/br/our-insights/all-insights/consumidores-esperam-interacoes-personalizadas. Acessado em 09/12/2024.

[237] Disponível em https://www.pwc.com.br/pt/estudos/setores-atividades/produtos-consumo-varejo/2023/GCIS_Pulse_6_PUB_Setembro_2023.pdf. Acessado em 12/12/2024.

[238] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acessado em 08/12/2024.

[239] Deve ser considerado a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento.

Verifica-se, portanto, que o conceito de dado pessoal é bastante abrangente, incluindo não apenas informações que claramente identificam uma pessoa natural – como nome completo e CPF, mas também dados a ela relacionados, que permitam a sua identificação – como profissão, idade, preferências, histórico de buscas ou compras, identificadores digitais.

Além disso, a LGPD estabelece expressamente que são dados pessoais aqueles *"utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada" (*, art. 12, §2º). Sendo assim, as preferências e os interesses atrelados ao perfil de uma pessoa são considerados dados pessoais sempre que possam ser associados a um indivíduo ou a um dispositivo e, nesse caso, aplicam-se os preceitos da LGPD. É necessário entender, dessa forma, se as preferências e os interesses associados ao perfil de uma pessoa, mesmo quando sua identidade é desconhecida, ainda são capazes de possibilitar sua identificação ou individualização.

A LGPD não traz, contudo, a definição de "perfil". Sendo assim, podemos tomar como base a definição do artigo 4.º, ponto 4, do General Data Protection Regulation, de acordo com o qual significa "*qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações*"[240].

Tendo em vista os pontos mencionados acima, cabe avaliar, no contexto das atividades de publicidade personalizada, quais os envolvidos na cadeia de tratamento dos dados para tal finalidade de fato conseguem associar um perfil a uma pessoa natural ou dispositivo específico, uma vez que, em alguns casos, é possível que o usuário não seja identificável, em decorrência da adoção de medidas técnicas, por exemplo.

Ademais, considerando o papel efetivamente exercido por cada uma das empresas na cadeia de tratamento de dados, há que se verificar o enquadramento como controlador ou operador, a fim de determinar as responsabilidades de cada um dos agentes em conformidade com a legislação – como, por exemplo, a adoção de base legal adequada, que cabe ao controlador. Relativamente às hipóteses legais para o tratamento de dados pessoais para fins de publicidade personalizada, entendemos que, no ordenamento jurídico brasileiro, o

240 Disponível em https://gdpr-info.eu/. Acessado em 13/12/2024.Acessado em 08/12/2024.

legítimo interesse é considerado a base legal mais adequada, ressalvando-se, no entanto, a necessidade de análise em cada caso concreto específico. Deve ser observado, dessa forma, o disposto no art. 10 da LGPD, e há que se balancear os interesses do controlador ou de terceiro e os direitos fundamentais e as liberdades do titular, ponderando-se se as finalidades são legítimas a partir de situações concretas.

Nesse sentido, a ANPD, em seu Guia Orientativo *"Hipóteses legais de tratamento de dados pessoais – Legítimo Interesse",* publicado em fevereiro de 2024[241], dispõe que *"o legítimo interesse do controlador ou de terceiro não pode ser usado como uma justificativa ampla e indefinida para condutas abusivas no tratamento de dados pessoais, que resultem em impactos excessivos e desproporcionais aos direitos dos titulares, sem as salvaguardas apropriadas. Em suma, é necessário que sejam equilibrados os interesses dos titulares e do controlador, levando em consideração seus direitos e liberdades fundamentais*". Outro ponto relevante é que deve ser garantida ao titular a transparência sobre tal tratamento, com informações claras, precisas e ostensivas e de acesso facilitado.

Nota-se que tema da publicidade personalizada ainda carece de regulamentação e esclarecimentos interpretativos, exigindo, assim, esforços adicionais, por parte do poder público, para que o tratamento de dados ocorra de forma transparente e idônea, garantindo mais segurança aos titulares e também às empresas.

O IAB Brasil, Associação de Mídia Interativa que desenvolve e fomenta a adoção de padrões técnicos e boas práticas na publicidade digital, em seu Código de Boas Práticas em Publicidade Digital[242] publicado em 2021, aduz que "*a publicidade baseada em dados sustenta a ideia de uma internet em que o acesso ao conteúdo é o mais aberto, livre e democrático possível. Sem a possibilidade do tratamento de Dados Pessoais, a publicidade seria menos relevante para os consumidores e haveria uma oferta menor de serviços oferecidos gratuitamente*".

Portanto, com o objetivo de apoiar o desenvolvimento de padrões técnicos e interpretativos sobre o tema, a seguir serão expostas algumas práticas e regulamentações adotadas por autoridades de proteção de dados em outras jurisdições.

[241]Disponível em https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf. Acessado em 08/12/2024.

[242] Disponível em https://iabbrasil.com.br/guia-codigo-de-boas-praticas-em-publicidade-digital/. Acessado em 10/12/2024.

3.2. Austrália

A autoridade de proteção de dados da Austrália, Office of the Australian Information Commissioner (OAIC), ressalta que *"a informação que um anunciante online coleta frequentemente não é suficiente identificar o usuário — pode ser apenas informações gerais sobre seus interesses e os sites que visitou. Assim, uma organização que utiliza publicidade direcionada pode não precisar cumprir as regras da Lei de Privacidade sobre como as informações pessoais são tratadas"*[243]. É imprescindível, portanto, verificar se os interesses vinculados a um perfil permitem ou não a identificação do titular, considerando o papel que cada agente de tratamento realiza na cadeia de publicidade digital.

Pode ser que, em alguns casos, determinado agente não possua, por exemplo, informações suficientes à identificação do usuário, por tratar apenas dados agregados ou não possuir informações adicionais, como identificadores on-line, que seriam necessárias à identificação indireta do usuário. Todavia, pode ser que, nesse mesmo caso, outro agente de tratamento possua informações adicionais e, assim, este consiga identificar os usuários por meio da combinação de dados.

Outro ponto que merece destaque é o consubstanciado nos Princípios de Privacidade Australianos, APP7, da OAIC, de acordo com o titular tem o direito solicitar ao agente de tratamento a identificação das fontes de seus dados pessoais tratados ou fornecidos a terceiros para fins de marketing direto, incluindo-se a publicidade direcionada nos exemplos mencionados no referido APP. As organizações apenas estariam dispensadas de fornecer tal informação caso *"seja impraticável ou irracional"* e, nesse caso, cabe a organização *"ser capaz de justificar que é impraticável ou irracional fornecer essa informação".* Destaca-se ainda, que não se pode deixar de responder a solicitação do titular apenas em razão do tempo e custos que seriam necessários, a não ser que seja possível demonstrar um ônus excessivo[244].

3.4. European Data Protection Boar Commission - EDPB

[243] Disponível em https://www.oaic.gov.au/privacy/your-privacy-rights/social-media-and-online-privacy/targeted-online-marketing. Acessado em 09/01/2025.

[244] Disponível em https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-7-app-7-direct-marketing. Acessado em 16/01/2025.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

O Comite Europeu para a Proteção de Dados (EDPB) é um organismo europeu independente. É a organização de cúpula que reúne as autoridades nacionais de proteção de dados dos países do Espaço Econômico Europeu, bem como a Autoridade Europeia para a Proteção de Dados (EDPS).

O EDPB visa assegura que o Regulamento Geral sobre a Proteção de Dados e a Diretiva relativa ao setor policial e judiciário sejam aplicados de forma coerente e assegura a cooperação, nomeadamente em matéria de supervisão.

O EDPB toma decisões vinculativas sobre casos transfronteiriços relativamente aos quais não se chegou a um consenso.

Sobre o tema de marketing e publicidade, no sentido de garantir o direito de acesso e de transparência ao titular de dados, pode servir como inspiração o disposto no documento "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679**",** do Working Party 29[245], o qual apresenta em seu Anexo I recomendações práticas, destacando-se a recomendação de que os controladores considerarem a implementação de mecanismo para que os titulares dos dados possam verificar seu perfil, incluindo detalhes das informações e fontes usadas para desenvolvê-lo.

Por sua, vez, nas "Diretrizes 8/2020 sobre o direcionamento para os utilizadores das redes sociais" [246], destaca-se que *"a mera utilização da palavra «publicidade» não seria suficiente para informar aos utilizadores de que a sua atividade está a ser monitorada para efeitos de publicidade direcionada"*.

Dessa forma, os titulares devem receber informações, de forma transparente e em linguagem facilmente compreensível, sobre a formação de perfil e o que significa, na prática, para o titular dos dados. Além disso, havendo mais de um agente na cadeia de tratamento de dados, deve ficar claro ao titular, no momento da coleta ou antes do início das atividades de tratamento, sobre a existência de várias fases e intervenientes no tratamento.

245 Disponível em https://ec.europa.eu/newsroom/article29/items/612053/en. Acessado em 10/12/2024.

246 Disponível em https://www.edpb.europa.eu/system/files/2021-11/edpb_guidelines_082020_on_the_targeting_of_social_media_users_pt_0.pdf. Acessado em 16/01/2025.

Além disso, consta nas Diretrizes 8/2020 que, havendo mais de um responsável pelo tratamento dos dados pessoais para fins de direcionamento de conteúdo e/ou serviços, especialmente em redes sociais, o nível de responsabilidade deve ser apurado conforme a efetiva função no tratamento e, para tanto, podem ser relevantes fatores como a capacidade de influenciar o tratamento, quais fases do tratamento são de responsabilidade de cada um dos agentes.

3.5. Reino Unido

A autoridade de proteção de dados do Reino Unido, Information Commissioner's Office (ICO), sobre a possibilidade ou não de identificação dos titulares a partir de um dado ou conjunto deles, recomenda que *"ao avaliar se um indivíduo é identificável, você deve considerar se os identificadores on-line, isoladamente ou em combinação com outras informações que podem estar disponíveis para aqueles que processam os dados, podem ser usados para distinguir um usuário de outro, possivelmente pela criação de perfis dos indivíduos para identificá-los"*[247]. Ainda, a autoridade orienta que, caso existam dúvidas sobre a possibilidade de identificação do indivíduo, seja adotada a boa prática de tratar as informações coletadas como se fossem dados pessoais, inclusive com a adoção de medidas de segurança adequadas e informações aos titulares sobre a coleta dos dados.

Ademais, no que tange ao marketing direto, a ICO adverte que, no Reino Unido, o "*soft-opt in*" - termo usado quando uma organização envia e-mails ou textos de marketing utilizando dados de clientes que foram coletados no momento em que este efetuou compra ou demonstrou interesse em produtos ou serviços -, somente pode ser usado para oferta de produtos e serviços semelhantes e, portanto, restringe-se aos casos de vendas ou negociações, trazendo o seguinte exemplo: "*se um cliente comprar um carro de você e lhe der seus detalhes de contato, você só poderá comercializar para ele coisas relacionadas ao carro, por exemplo, oferecendo serviços ou MOTs (*inspeções veiculares*)"*[248].

247 Disponível em https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-data/what-are-identifiers-and-related-factors/#:~:text=These%20include%3A,tell%20you%20something%20about%20them. Acessado em 09/01/2025.

248 Disponível em https://ico.org.uk/for-organisations/advice-for-small-organisations/frequently-asked-questions/marketing/#whensoft. Acessado em 16/01/2025.

Especificamente no que concerne ao tratamento de dados pessoais de crianças no ambiente online, a ICO, em seu "Age appropriate design: a code of practive for online services"[249] publicado em 2021, estabelece normas e faz recomendações práticas para garantiria dos melhores interesses da criança. Dentre tais pontos, destacam-se, além da elaboração de RIPD para avaliação e mitigação de riscos:

i) Por padrão, as configurações das aplicações devem ser de "alta privacidade" e devem ser desativadas opções de geolocalização e perfilamento, a não ser que existam razões que demonstrem a necessidade configuração padrão distinta, levando em conta o melhor interesse da criança. Além disso, quando a geolocalização estiver ativa, deve haver um aviso óbvio para crianças. No que tange ao perfilamento, apenas deve ocorrer se forem adotadas medidas apropriadas para proteção da criança de quaisquer efeitos nocivos.

ii) Havendo a ferramenta de controle parental, a criança deve ser informada por um aviso apropriado à sua idade. Caso tal ferramenta permita monitoramento de atividade on-line ou a localização em que a criança se encontra, deve haver um aviso óbvio para crianças enquanto ela estiver sendo monitorada.

iii) Em jogos ou outros aplicações interativas, deve ser evitada a coleta de dados pessoais na forma de incentivo ao engajamento, por exemplo, vantagens personalizadas em jogos (apoiado no uso individual de seus dados pessoais), em troca de tempo prolongado no jogo.

Tais medidas práticas, dispostas no Código da ICO, contribuem ao respeito da privacidade e desenvolvimento do público infantil e adolescente durante suas interações no ambiente digital.

3.6. SRO´s – Self Regulation Autorities

a) Brasil: Conselho Nacional de Autorregulamentação Publicitária (CONAR)

No cenário nacional, o Código Brasileiro de Autorregulamentação Publicitária (CBAP) do CONAR, de 1980, prevê, em seu artigo 19, que "*toda atividade publicitária deve caracterizar-se pelo* ***respeito à dignidade da pessoa humana, à intimidade,*** *ao interesse social, às instituições e símbolos nacionais, às autoridades*

[249] Disponível em https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/. Acessado em 13/12/2024.

constituídas e ao núcleo familiar". Nota-se, portanto, que para contribuir para o bem-estar social e a construção de uma sociedade justa e equilibrada, a publicidade deve respeitar os direitos e os limites individuais.

A temática da privacidade e uso de dados para publicidade já é analisado pelo CONAR há alguns anos, sendo certo que a autorregulação do setor publicitário pode contribuir para a adoção de práticas de conformidade para o uso ético de dados pessoais, ao estabelecer diretrizes e boas práticas em complemento à Lei Geral de Proteção de Dados e seus regulamentos, tal como ocorre em outros países, como se verá a seguir. O estímulo à conformidade, partindo da própria entidade responsável pela autorregulamentação do setor, é essencial para a manutenção da publicidade baseada em dados pessoais, a fim de tornar o ambiente digital mais confiável e seguro para os usuários, o que, por sua vez, reforçará a confiança nas plataformas e nas marcas envolvidas.

A seguir, portanto, serão apresentadas boas práticas e regulamentos resultantes da autorregulação no exterior, que podem servir como inspiração para o incentivo desse mecanismo no Brasil.

b) International Chamber of Commerce (ICC)

No cenário internacional, o Código de Comunicação de Marketing e Publicidade da ICC, Câmara de Comércio Internacional, é um marco que orienta práticas responsáveis de marketing e publicidade. Ele serve como base para quase 50 códigos de autorregulação em diversos países.

A ICC acredita que um programa robusto e eficiente de autorregulação da publicidade pode beneficiar tanto os consumidores quanto a indústria publicitária, ao promover a publicidade responsável e condições equitativas entre os concorrentes, com base em um padrão comum. Dessa forma, contribui para a proteção dos consumidores ao mesmo tempo em que favorece a liberdade criativa[250].

[250] Disponível em https://iccwbo.org/wp-content/uploads/sites/3/2020/06/2020-icc-srtoolkit-benefits-of-sr.pdf. Acessado em 16/01/2025.

O Código de Comunicação de Marketing e Publicidade da ICC[251], em seu art. 22, determina que o tratamento de dados pessoais deve respeitar a privacidade dos indivíduos, ser não excessivo, ser claro e transparente e, ainda, devem ser respeitas as preferências expressas dos indivíduos. Havendo tratamento de dados pessoais de crianças, as informações devem ser apropriadas à idade.

Especificamente no que tange à publicidade baseada em interesses, o artigo C17 estabelece que devem ser adotadas medidas específicas, que sejam fáceis de usar, acessíveis e intuitivas, para garantia da transparência, fornecendo aviso claro e visível sobre a coleta de dados para esta finalidade. Há recomendação de que tal aviso faça referência às diretrizes de autorregulação relevantes e às melhores práticas em cada jurisdição.

c) França: Autoridade de Regulação de Profissionais da Publicidade da França ARPP

A ARPP, Autoridade de Regulação de Profissionais da Publicidade da França, tem como base para construção de seus próprio Códigos e regulamentos o Código de Comunicação de Marketing e Publicidade da ICC. Em seu *Recommandation Communication Publicitaire Numérique V5*[252]*,* a ARPP determina que "*a natureza comportamental de uma comunicação publicitária digital deve ser identificável*", por meio do uso de "*símbolo visível específico, distinguível do conteúdo da mensagem e perfeitamente legível, pode informar o público sobre a natureza comportamental de uma comunicação publicitária digital*". Além disso, a Autoridade recomenda que, a partir do referido símbolo, estejam disponíveis ao usuário as especificações sobre a publicidade, inclusive acerca das informações coletadas sobre o titular e condições da segmentação.Também há recomendação de que seja disponibilizada, nesse mesmo espaço, a possibilidade de aceite ou não de *cookies* de navegação e, ainda, a alternativa de oposição a qualquer publicidade comportamental[253].

---

[251]Disponível em https://iccwbo.org/wp-content/uploads/sites/3/2024/09/ICC_2024_MarketingCode_2024.pdf. Acessado em 12/01/2025.

[252]Disponível em*https://www.arpp.org/nous-consulter/regles/regles-de-deontologie/digital-advertising-and-marketing-communications-code/*. Acessado em 09/12/2024.

[253]"La nature comportementale d'une communication publicitaire numérique doit pouvoir être identifiée comme telle. A ce titre, l'utilisation d'un symbole spécifique apparent, distinguable du contenu du message et parfaitement lisible peut permettre d'informer le public sur la nature comportementale d'une communication publicitaire numérique.

A recomendação da ARPP francesa de inclusão um símbolo visível e específico sobre a publicidade personalizada é uma medida que garante ao titular devida transparência sobre o tratamento de seus dados. Ademais, a orientação de que o referido símbolo seja "*distinguível do conteúdo da mensagem*" e "*perfeitamente legível*" é crucial para garantir que o público compreenda a diferença entre o conteúdo editorial e as ações publicitárias, contribuindo para o fortalecimento da ética na publicidade. No que tange à recomendação de alternativa de oposição específica à publicidade comportamental, cujo acesso deve constar junto ao referido símbolo, ao facultar que os indivíduos possam escolher não ser alvo desse tipo de marketing de forma facilitada, garante-se à autonomia e o controle por parte do titular sobre o tratamento de seus dados pessoais.

Ainda, em atenção à privacidade infantil, a ARPP veda, no art. art. 9, b do referido Código, que dados comportamentais de menores de 13 anos sejam usados para publicidade personalizada, ou seja, de acordo com o órgão regulador, a criação de categorias específicas de segmentação publicitária somente pode ser direcionada aos maiores de 13 anos[254].

d) Espanha: AUTOCONTROL

Por sua vez, o denominado AUTOCONTROL, que é o organismo independente de autorregulação da indústria publicitária na Espanha, em seu "Código de Conducta para el Tratamiento de Datos en la Actividad Publicitaria" de 2023[255], reforça o dever sobre a informação ao titular de dados e, ainda, dispõe que a informação pode ser fornecida em camadas, por meio de textos expansíveis, por exemplo, a fim de melhorar a

---

Il est de plus recommandé de permettre au public, par un accès en un simple clic sur le symbole susvisé à un espace dédié et spécifique, de s'informer des spécificités inhérentes à ce type de publicité (nature des informations recueillies, modalités d'utilisation à des fins de ciblage comportemental…).
Cet espace dédié doit également offrir au public des informations claires sur les différentes possibilités permettant de refuser ou d'accepter l'affichage de publicité comportementale, notamment des modalités :

- d'acceptation ponctuelle ou permanente à l'implantation de témoins de navigation (ou cookies) (paramétrage du navigateur),
- de suppression des témoins de navigation (ou cookies),
- d'opposition à l'affichage de toute publicité comportementale auprès des prestataires de publicité comportementale".

[254] "Les professionnels s'interdisent de créer des catégories spécifiques de ciblage publicitaire correspondant aux centres d'intérêt des enfants dont l'âge est inférieur ou égal à 13 ans" .

[255] Disponível em https://www.autocontrol.es/wp-content/uploads/2023/10/codigo-de-conducta-proteccion-de-datos-autocontrol.pdf. Acessado em 12/12/2024.

transparência e evitar sobrecarga de informações ao titular. Caso ocorram mudanças no tratamento de dados para fins publicitários, a cláusula informativa deve ser atualizada e fornecida com as modificações claras e, alternativamente, há recomendação de que seja fornecido um resumo das alterações, trazendo o exemplo abaixo:

> *"Exemplo: Uma notificação da alteração da cláusula informativa poderia ser a seguinte (as alterações estão marcadas em negrito): "Manteremos um registro dos produtos que você visualiza e compra em nossa loja online,* ***assim como das consultas que você nos faz sobre nossos produtos,*** *para mostrar publicidade e recomendações de produtos em nosso site com base nos seus interesses, que identificamos com base nos produtos que você vê, compra* ***ou consulta****".*
>
> *Um resumo sobre a modificação da cláusula informativa anterior poderia ser o seguinte: "Além de continuarmos a considerar os produtos que você visualiza e compra em nossa loja online* ***para ajustar nossa publicidade aos seus interesses****, a partir de agora também levaremos em conta os* ***produtos sobre os quais você nos consulta*** *(por exemplo, perguntando sobre sua disponibilidade ou tamanhos)"*[256]*.*

No exemplo em questão, a comunicação informa claramente ao titular que, além das informações anteriormente coletadas para publicidade personalizada, a empresa passou a coletar, também, informações sobre os produtos pesquisados, garantindo, assim, maior transparência e controle sobre o uso dos dados pessoais, além de assegurar o cumprimento da legislação de proteção de dados.

Além disso, o referido Código do AUTOCONTROL, em seu item 7.5, dispõe sobre listas de oposição, ou seja, o titular pode se cadastrar em listas se desejar não receber comunicações diretas de marketing. Sendo assim, as empresas devem observar tais listas, havendo somente duas exceções: i) receber o consentimento específico do titular para realizar comunicações de marketing direto; ii) possuir relação contratual prévia, desde

[256] Redação original: Ejemplo: Una notificación del cambio de cláusula informativa podría ser la siguiente (los cambios se marcan en negrita): "Llevaremos un registro de los productos que visualizas y compras en nuestra tienda online, **así como de las consultas que nos hagas sobre nuestros productos**, para mostrarte publicidad y recomendaciones de productos en nuestro sitio web en base a tus intereses, que identificamos en base a los productos que ves o compras, **o sobre los que nos consultas**". Un resumen sobre la modificación de la cláusula informativa anterior podría ser el siguiente: "Además de seguir teniendo en cuenta los productos que visualizas y compras en nuestra tienda online **para ajustar nuestra publicidad a tus intereses**, a partir de ahora también tendremos en cuenta los **productos sobre los que nos consultes** (por ejemplo, preguntando sobre su disponibilidad o tamaños)".

que os dados de contato do destinatário tenham sido obtidos de forma lícita e sejam usados para enviar comunicações comerciais referentes a produtos ou serviços da sua própria empresa, semelhantes aos inicialmente contratados pelo cliente[257]. A primeira exceção está prevista no Código de Conduta do AUTOCONTROL, onde também há menção à segunda, a qual é expressamente prevista no artigo 21.2 da Lei conhecida como "LSSI" ou "Lei da Internet"[258]. Em qualquer dos casos, o titular tem o direito de se opor ao recebimento de comunicações de marketing direto.

Embora existam diferenças legislativas e regulatórias entre os exemplos espanhol e francês e a legislação brasileira, há pontos que podem servir de inspiração para o desenvolvimento de boas práticas no Brasil, especialmente no que diz respeito à promoção de ações mais transparentes, éticas e alinhadas à legislação de proteção de dados. Essas práticas podem promover o controle dos titulares sobre o uso de seus dados pessoais, além de fortalecer a confiança nas estratégias de marketing.

4. Meios para aumentar a proteção de dados e segurança jurídica:

Diante do cenário evidenciado nas seções anteriores, resta claro que, cada vez mais, os dados pessoais impulsionam práticas de marketing e publicidade, especialmente no meio digital. É essencial, portanto, que tal tratamento de dados ocorra em conformidade com a Lei e, ainda, sejam fomentadas boas práticas sobre o tema.

Neste sentindo, após avaliar práticas de conformidade adotadas em diversos países e, inclusive, no ambiente de autorregulação, esta seção tem como principal objetivo apontar práticas e tecnologias que podem

[257] "Las entidades adheridas que pretendan realizar comunicaciones de mercadotecnia directa deberán consultar previamente los sistemas de exclusión publicitaria que afecten a su actuación (por ejemplo, listas Robinson), para excluir del tratamiento a los interesados que hayan manifestado su negativa al mismo. Para cumplir esta obligación, bastará con consultar los sistemas de exclusión incluidos en la relación publicada por la autoridad de control competente en su sede electrónica.
La consulta a estos sistemas de exclusión no será necesaria si el afectado hubiera prestado su consentimiento para recibir la comunicación a quien pretenda realizarla o el responsable pudiera ampararse en la excepción prevista en el artículo 21.2 de la LSSI."

[258] Disponível em https://www.boe.es/eli/es/l/2002/07/11/34/con. Acessado em 12/12/2024.

ser implementadas e fomentadas no cenário brasileiro, para fortalecimento da proteção de dados e da segurança jurídica e, consequentemente, promoção da inovação alinhada às garantias fundamentais dos titulares e à harmonização normativa.

Cabe destacar, nesse contexto, a relevância do papel da Autoridade Nacional de Proteção de Dados, a quem compete não apenas fiscalizar e aplicar sanções em caso de tratamento realizado em desacordo com a legislação, como também zelar pela proteção de dados, promover na população o conhecimento sobre o tema, propor estudos e editar normas, regulamentos e procedimentos, dentre outras atribuições elencadas no art. 55-J da LGPD.

É certo que os guias e recomendações práticas da ANPD ajudam a estabelecer padrões de conformidade e, ainda, ao firmar entendimentos interpretativos sobre a legislação e suas aplicações, harmonizam as práticas de mercado. Nesse sentido, faz-se necessário que a Política Nacional, em atenção ao tema do tratamento de dados para fins de marketing e publicidade, estimule à ANPD à elaboração de estudos e guias específicos sobre o assunto, a fim de zelar pela privacidade dos indivíduos e, ao mesmo tempo, impulsione ferramentas práticas para que o setor publicitário consiga operar dentro dos limites legais, sem perder sua capacidade de inovar e competir.

Dentro dessa temática, alguns pontos merecem atenção especial e poderiam ser abordados pela ANPD em guias específicos direcionados ao setor publicitário, como, por exemplo:

- A definição de “perfil”, tal como ocorre no GDPR, já que a LGPD não apresenta tal conceituação;
- Orientações e boas práticas a fim de garanta da transparência, tal como indicado pela ARPP francesa, para inclusão de símbolo visível e específico sobre a natureza comportamental de determinada comunicação; bem como sobre a informação ao titular a respeito das fontes utilizadas para o desenvolvimento de perfil, conforme pontuado pela OAIC, na Austrália, e EDPB, na União Europeia;
- Limites do perfilamento e indicação de práticas para evitar tratamento de dados pessoais de forma discriminatória ou excludente, bem como a indicação do que pode ser considerado discriminatório ou excludente;
- Condições e boas práticas específicas em relação ao tratamento de dados de crianças e adolescentes, estimulando a adoção configurações de “alta privacidade” por padrão,

conforme apontado pela ICO, bem como o desestímulo à segmentação, para fins publicitários, de dados de crianças, como estipulado pela ARPP.

Além disso, a adoção de uma página informativa pela ANPD, no formato de perguntas e respostas, poderia trazer esclarecimentos importantes e de forma simplificada sobre o tema, os quais seriam úteis não somente ao setor empresarial, como também aos titulares. Nesse caso, poderiam ser abordados temas como a possibilidade ou não de identificação dos titulares a partir dos dados pessoais tratados, a exemplo das práticas adotas pela autoridade de proteção de dados australiana, OAIC[259], e pela ICO, do Reino Unido[260], em seus respectivos sites.

Certamente, as atividades de conscientização da população por parte da ANPD também merecem destaque, a fim de promover esclarecimentos e a facilitação da compreensão de conceitos provenientes da legislação. Por meio de iniciativas educacionais periódicas, será possível garantir que os indivíduos tomem decisões com mais autonomia, cientes de seus direitos e das consequências de sua escolhas ou interações no meio online, por exemplo.

Portanto, além de guias específicos direcionados ao setor publicitário, é necessário que a ANPD também direcione esforços à promoção de atividades que proporcionem a conscientização dos titulares de dados. Tais práticas, voltadas à população, permitem que diversos grupos sociais conheçam seus direitos e, ainda, participem ativamente da construção de políticas públicas eficazes, contribuindo, assim, para o fortalecimento das instituições e da convivência social.

No cenário internacional, resta claro que as entidades autorreguladoras possuem importante papel na orientação de práticas responsáveis de marketing e publicidade, a exemplo da atuação da ICC, e também da ARPP e AUTOCONTROL, conforme pontuado na seção 3.6. No Brasil, o Conselho Nacional de Autorregulação Publicitária (CONAR) já desempenha um papel relevante, mas as questões relacionadas ao tratamento de dados pessoais demandam iniciativas adicionais, voltadas, por exemplo, às boas práticas sobre a coleta ética de dados, medidas de transparência e possíveis restrições ao uso de técnicas de profiling que sejam demasiadamente invasivas, inclusive por faixa etária.

[259] 3.2
[260] 3.5

Nesse cenário, a Política Nacional de Proteção de Dados poderia estimular a cooperação e a parceria estratégica, entre a ANPD e o CONAR, para o desenvolvimento de ações conjuntas que promovam a segurança e a conscientização sobre boas práticas no setor de publicidade e marketing.

Isso porque, ao mesmo tempo em que há um importante papel do Estado e da ANPD na regulação deste tema, as questões técnicas e estruturas de governança já existentes demandam uma abordagem específica do ambiente regulatório.

Cabe destacar, inclusive, que o Guia para Elaboração de Análise de Impacto Regulatório (AIR), emitido pelo Ministério da Economia brasileiro[261], cujo objetivo é trazer elementos da boa prática regulatória aos órgãos e às entidades da administração pública federal direta, autárquica e fundacional, recomenda que, sempre que possível, sejam adotadas ações não normativas.

Ao expor as alternativas não normativas, o referido Guia adota a classificação utilizada pela Organização para a Cooperação e Desenvolvimento Econômico - OCDE, dentre a qual se destaca no presente caso, a corregulação, assim definidas no Guia:

> *"Corregulação: ou regulação compartilhada, ocorre quando a indústria desenvolve e administra seus próprios padrões, mas o governo fornece o apoio legal para permitir que eles sejam aplicados. Em geral, o governo determina padrões ou parâmetros de qualidade ou performance, permitindo que os atores escolham a melhor forma de adequar seus produtos, processos, serviços ou tecnologia de modo a atender o desempenho esperado."*

Nesse caso, portanto, há participação ativa e necessária dos interessados na solução, o que pode trazer como benefício maior compreensão e adesão por parte do setor regulado, além de ser uma alternativa menos onerosa ao Estado para a minimização de eventuais deficiências regulatórias.

[261]Disponível em https://www.gov.br/mma/pt-br/acesso-a-informacao/analise-air-e-arr/guia-para-elaboracao-de-air-2021.pdf. Acessado em 12 de janeiro de 2025.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANEXO XXVIX – ESTUDO DE CASO: SAÚDE

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ESTUDO DE CASO: SAÚDE

Conselheiro da ANPD: Rony Vainzof[262]

SUMÁRIO

[262] Conselheiro titular do CNPD. O trabalho contou com o apoio dos pesquisadores Verônica Barros e Mateus Lamonica.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

1. INTRODUÇÃO

1. Os avanços tecnológicos, com a crescente digitalização e aumento do tratamento de dados pessoais, permitem diagnósticos mais rápidos, precisos e personalizados, além de viabilizar uma gestão mais eficiente de serviços de saúde, com maior disponibilização e acessibilidade. A telemedicina e a medicina preditiva com suas inovações disruptivas são excelentes exemplos que demonstram a melhora significativa no atendimento e na qualidade de vida das pessoas. É neste cenário de inovação exponencial que surge a Saúde 4.0, também denominada Saúde Digital[263], um conceito que trata da aplicação em serviços médicos de recursos tecnológicos desenvolvidos pela indústria 4.0.

2. Todo esse contexto de evolução do setor, cada vez mais conectado e dependente da tecnologia, que permite a melhoria da qualidade de vida das pessoas, levanta também questões relevantes sobre como conciliar privacidade, proteção e segurança, principalmente por envolver dados pessoais sensíveis, com o desenvolvimento econômico, tecnológico e a inovação.

2. A IMPORTÂNCIA DO SETOR DA SAÚDE PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E INOVAÇÃO

3. Entre 2010 e 2017, a participação do setor de Saúde no PIB cresceu de 8% para 9,2%, somando R$ 608,3 bilhões em 2017. Desse total, 5,4% do PIB (R$ 354,6 bilhões) vieram de despesas das famílias e instituições sem fins lucrativos, enquanto 3,9% (R$ 253,7 bilhões) corresponderam a despesas do governo. Comparando estes valores com os gastos similares de outros países, tais como os da Organização para a Cooperação e Desenvolvimento Econômico (OECD), o Brasil tem nível semelhante ao Chile, Reino Unido e Grécia, mas, na despesa do governo, também relacionada ao PIB, situou-se um pouco abaixo da média.

---

[263] A Saúde Digital é um campo em constante crescimento e modernização nos últimos anos. No Brasil, a prática da telemedicina foi impulsionada a partir de 2020, durante a pandemia de Covid-19, tendo sido recentemente regulamentada pelo Conselho Federal de Medicina (CFM). De acordo com um artigo *do Wisconsin Institute for Healthcare Systems Engineering*, da Universidade de Wisconsin, nos Estados Unidos, a Saúde 4.0 é fundamentada em dois pilares principais: **(1)** Inteligência: envolve o uso de inteligência artificial (IA) para oferecer atendimento individualizado e centrado no paciente, aprimorando diagnósticos e tratamentos. A IA possibilita estratificação, classificação, análises preditivas, monitoramento e otimização de terapias; **(2)** Interconexão: promove a integração dos sistemas de Saúde, formando uma rede de informações que aumenta a eficiência dos processos. A tecnologia conecta equipes médicas entre si e com os pacientes, sistemas de custos e seguros, dispositivos e sensores médicos, dados históricos, instituições de Saúde e muito mais.
PORTAL TELEMEDICINA. O futuro da saúde digital: o que esperar de 2023. Disponível em: https://portaltelemedicina.com.br/o-futuro-da-saude-digital-o-que-esperar-de-2023.

4. No mesmo período acima citado, o valor adicionado pelo setor de Saúde na economia brasileira aumentou de 6,1% para 7,6%. A participação do setor no total de empregos cresceu de 5,3% para 7,1%, e sua contribuição para remunerações passou de 8,3% para 9,6%.

5. Esses dados reforçam a crescente relevância do setor de Saúde como gerador de renda, emprego e impacto econômico e demonstram a forte tendência à expansão. Para tanto, é fundamental o incentivo à interoperabilidade dos dados incluindo aqueles provenientes do setor público, viabilizando a integração lícita, segura e responsável de informações de diferentes fontes, o que possibilitará análises abrangentes que orientem políticas públicas mais eficazes e fomentem a pesquisa científica, impulsionando, assim, o bem-estar da coletividade.

6. A preocupação do país com o setor da Saúde é também percebida nas inúmeras políticas públicas existentes em todas as esferas da federação. No âmbito nacional, as iniciativas e os planos governamentais incentivam a digitalização e o uso de tecnologias para impulsionar os serviços de saúde fornecidos, conforme destacado abaixo.

Estratégia Brasileira de Transformação Digital (E-Digital)[264]

7. A E-Digital, como o próprio nome sugere, busca estimular o desenvolvimento digital do Brasil, promovendo a inclusão, a inovação, a competitividade e o crescimento econômico sustentável do país. Capitaneada pelo do Ministério da Ciência, Tecnologia e Inovação (MCTI), a Estratégia foi estruturada em eixos principais que trazem aspectos relevantes para o setor da Saúde:

[264] Criada originalmente em 2018, pela Portaria MCTIC nº 1.556/2018, a E-Digital foi atualizada para o período 2022-2026 e aprovada através da Portaria nº 6.543/2022, do Ministério da Ciência, Tecnologia e Inovação (MCTI). Portanto, a E-Digital, permanece válida até sua próxima revisão. Ela surgiu como integrante do Sistema Nacional para a Transformação Digital, instituído pelo Decreto nº 9.319/2018, que trouxe a estrutura de governança para a implantação E-Digital. Este Decreto nº 9.319/2018 foi recentemente revogado pelo Decreto nº 12.308, de 11 de dezembro de 2024, que simplificou a estrutura governamental e manteve apenas o Comitê Interministerial para a Transformação Digital (CITDigital), com objetivo de assessorar o Presidente da República na elaboração, na implementação e no acompanhamento de políticas públicas destinadas à transformação digital.
BRASIL. Ministério da Ciência, Tecnologia e Inovação. E-Digital: Ciclo 2022-2026. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosestrategiadigital/e-digital_ciclo_2022-2026.pdf.

- Eixo Habilitador B. Pesquisa, Desenvolvimento e Inovação:

  - Promover PD&I, inclusive por meio de encomendas tecnológicas governamentais, em temas estratégicos para a transformação digital, como Internet das Coisas (IoT), em áreas como a Saúde;
  - Estimular investimentos públicos e privados em PD&I ligados às demandas prioritárias da Saúde 4.0.

- Eixo de Transformação Digital F. Transformação Digital da Economia:

  - F1. Economia baseada em dados:
    - Aprimorar a política de dados abertos do Poder Executivo Federal, envolvendo todos os entes federados e a sociedade civil;
    - Incentivar e financiar a interoperabilidade e processos baseados em dados e a cocriação de ferramentas, sistemas e plataformas;
    - Promover a padronizar das formas de acesso e oferta de dados públicos.

  - F2. Um mundo de dispositivos conectados:
    - Fomentar o desenvolvimento e a implantação de ambientes/plataformas para validação e avaliação das soluções de Internet das Coisas (IoT), especialmente para a Saúde 4.0;
    - Promover e fomentar a escalabilidade e a replicabilidade das plataformas abertas nacionais de IoT, *hardware*, aplicação em PD&I e empreendedorismo nos setores priorizados no plano de IoT, que inclui a Saúde;
    - Incentivar formatos inovadores de ofertas de produtos e serviços digitais e robótica, tais como plataformas IoT abertas e *Robot as a Service* (RaaS) em setores como a Saúde.

8. Além das ações mencionadas, a E-Digital destaca a importância do uso de tecnologias digitais na Saúde para (i) simplificar processos burocráticos de acesso à informação e cidadania; (ii) otimizar investimentos; (iii) realocar servidores para áreas que demandam ações estratégicas. Ao mesmo tempo, aponta para a necessidade

de alguns desafios a serem superados na área da Saúde, como a falta de acesso à tecnologia e a necessidade de investimentos direcionados para o desenvolvimento de tecnologias.

9. Por fim, a E-Digital enfatiza que a transformação digital na Saúde depende da participação ativa do Brasil em processos decisórios internacionais, incluindo marcos regulatórios e normas tecnológicas.

Estratégia Nacional de Governo Digital[265]

10. A Estratégia Nacional de Governo Digital para o período de 2024 a 2027 tem como objetivo geral a busca de um Estado mais inclusivo, eficaz, proativo, participativo e sustentável, para o que destaca expressamente a Saúde, direito social fundamental, garantido à coletividade pelo artigo 6º da Constituição Federal[266]. Dentre suas ações, estabelece a necessidade (i) de oferta de soluções que atendam às necessidades da sociedade e reconheçam as desigualdades sociais e as barreiras de acesso aos serviços públicos; (b) da adaptação de seus processos às demandas atuais da sociedade, com inovação, uso adequado de tecnologias, reuso seguro de dados e melhor aplicação dos recursos públicos; e (iii) da transparência, do acesso à informação, da participação social na formulação de políticas públicas e da promoção do desenvolvimento sustentável.

11. Como uma das ações de transformação digital prioritárias da administração pública federal, a Estratégia traz a importância de iniciativas de transformação digital das políticas e dos serviços públicos de Saúde[267], reconhecendo a necessidade de crescente utilização de dados pessoais e o cuidado que se deve ter com a licitude de seu tratamento. Por isso destaca, em seu "Objetivo 4" a relevância da "ampliação da resiliência e da maturidade das estruturas tecnológicas governamentais com atenção à privacidade, proteção de dados

[265] Está prevista na Lei nº 14.129, de 29 de março de 2021 (Lei do Governo Digital), mas foi instituída pelo Decreto nº 12.069, de 21 de junho de 2024 (art. 7º). A Portaria SGD/MGI nº 4.248, de 26 de junho de 2024 estabelece recomendações para o alcance dos objetivos para o período de 2024 a 2027.
BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Estratégia Nacional de Governo Digital. Disponível em: https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/estrategianacional

[266] "Art. 6º. São direitos sociais a educação, a Saúde, a alimentação, o trabalho, a moradia, o transporte, o lazer, a segurança, a previdência social, a proteção à maternidade e à infância, a assistência aos desamparados, na forma desta Constituição."
BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

[267] Estratégia Nacional de Governo Digital, artigo 10.

pessoais, segurança da informação e segurança cibernética", prevendo como medidas fundamentais as que seguem:

> "4.1 Instituir estrutura de governança e coordenação para implementação de medidas de reforço à privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética, em articulação com estruturas de mesmo propósito de âmbito regional e nacional;
> 4.2 Estabelecer plano de ação de reforço à privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética que contemple diagnóstico, controles, metodologias e soluções tecnológicas adequadas aos riscos identificados;
> 4.3 Designar encarregado pelo tratamento de dados pessoais e gestor de segurança da informação;
> 4.4 Promover ações de sensibilização, conscientização e capacitação para agentes públicos, lideranças governamentais e sociedade sobre privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética."

12. Ademais, em seu **"Objetivo 5"**, demonstra a essencialidade do tratamento de dados, inclusive pessoais, ao exigir a qualificação da **"tomada de decisões e a oferta de serviços nas organizações públicas com o reuso constante e de forma ética dos dados disponíveis para análises, interoperabilidade e personalização**", estabelecendo a relevância de:

> "5.1 Elaborar, publicar e implementar um programa de governança de dados;
> 5.2 Estabelecer e adotar mecanismos de interoperabilidade e compartilhamento de dados, entre os órgãos e com outros entes federados, especialmente os ofertados pela Plataforma GOV.BR, para qualificação das políticas públicas e eliminação de pedidos de dados dispensáveis na oferta de serviços públicos;
> 5.3 Contribuir para a elaboração e adotar um modelo de compartilhamento de dados que permita ao cidadão o uso seguro dos seus dados e melhore sua experiência no acesso a serviços;
> 5.4 Estimular o uso e a adoção de análise de dados, de maneira ética, na tomada de decisão das políticas públicas e na personalização dos serviços."

13. Já seu "Objetivo 6" trata da disposição de "infraestrutura moderna, segura, escalável e robusta para a implantação e evolução de soluções de governo digital, promovendo soluções estruturantes compartilhadas, uso de padrões comuns e a integração entre os entes federados", medidas essenciais para a Saúde, eis que se

trata de um direito cujas competências administrativa[268] e legislativa[269] são comuns, ou seja, repartidas entre todas as esferas da federação (União, Estados, Distrito Federal e Municípios).

14. Por fim, o "Objetivo 7" da Estratégia, busca "estimular e fomentar o desenvolvimento do ecossistema de inovação e de governo digital, envolvendo todos os entes federados e a sociedade, gerando novas oportunidades para o aprimoramento do setor público e desenvolvimento de negócios, inclusive para o desenvolvimento e o uso de tecnologias emergentes".

Plano Nacional de Internet das Coisas[270]

15. Por sua vez, o Plano Nacional de Internet das Coisas ("Plano Nacional IoT") visa implementar e desenvolver a Internet das Coisas (IoT) no Brasil, promovendo a livre concorrência e a circulação de dados com segurança. Seus objetivos incluem melhorar a qualidade de vida, capacitar profissionais, aumentar a produtividade das empresas, fomentar parcerias público-privadas e integrar o Brasil no cenário internacional, para o que, mais uma vez, se destaca o setor da Saúde.

- Incentivos do Plano com reflexos na Saúde:
    - Melhoria de vida e eficiência: visa melhorar a qualidade de vida e promover eficiência nos serviços por meio da IoT. (Art. 3º, I);
    - Prioridade para Saúde: os ambientes de Saúde são prioritários para aplicação de soluções de IoT (Art. 4º). São considerados critérios de oferta, demanda e capacidade de desenvolvimento local. (Art. 4º, §1º).

- Necessidade de tratamento de dados pessoais conforme reconhecido no Plano:

[268] Constituição da República Federativa do Brasil. "Art. 23. É competência comum da União, dos Estados, do Distrito Federal e dos Municípios: (...) II- cuidar da Saúde e assistência pública, da proteção e garantia das pessoas portadoras de deficiência;"
[269] Constituição da República Federativa do Brasil. "Art. 24. Compete à União, aos Estados e ao Distrito Federal legislar concorrentemente sobre: (...) XII- previdência social, proteção e defesa da Saúde;"
[270] Instituído pelo Decreto nº 9.854 de 2019.
BRASIL. Ministério da Ciência, Tecnologia e Inovação. Internet das Coisas. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/internet-das-coisas

- **Livre circulação de dados:** é a finalidade do Plano, mas deve observar as diretrizes de segurança da informação e proteção de dados pessoais (Art. 1º);
- **Serviços de valor adicionado:** incentiva o desenvolvimento de serviços de valor adicionado, que por sua vez, implicam o tratamento de dados pessoais. (Art. 2º, IV);
- **Regulação, segurança e privacidade:** o plano de ação para viabilizar o Plano Nacional de IoT inclui o tema "regulação, segurança e privacidade" (Art. 5º, IV);

Estudo de IoT[271]e Aprofundamento de Verticais – Saúde

16. Apoiado pelo Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), em parceria com o Banco Nacional de Desenvolvimento Econômico e Social (BNDES), esse Estudo buscou diagnosticar o ecossistema brasileiro de IoT e propor políticas públicas para sua implementação. Foi composto por 4 fases, sendo o setor da Saúde examinado na fase 3. Nela foi elaborado o "Relatório de aprofundamento das verticais – ambiente de Saúde", cujas principais considerações foram destacadas abaixo.

Produto 7B: Aprofundamento de Verticais – Saúde[272]:

17. Apresenta um plano de ação para a implementação de Internet das Coisas (IoT) no setor de Saúde brasileiro. Ele analisa os desafios do sistema de Saúde, explora aplicações da IoT para melhorar a qualidade de vida e a eficiência da gestão, identifica as tecnologias necessárias e mapeia as barreiras para adoção, culminando em uma visão estratégica para o desenvolvimento e implementação de soluções de IoT em Saúde no país. O Relatório inclui estudos de caso de aplicações específicas e uma análise da capacidade tecnológica brasileira nesse setor. Neles são trazidos:

- Principais Desafios: A Saúde é uma das principais preocupações dos brasileiros. O sistema de Saúde enfrenta desafios como a tripla carga de doenças (crônicas, infectocontagiosas e de causas

[271] BANCO NACIONAL DE DESENVOLVIMENTO ECONÔMICO E SOCIAL (BNDES). Estudo Internet das Coisas (IoT): um plano de ação para o Brasil. Disponível em: https://www.bndes.gov.br/wps/portal/site/home/conhecimento/pesquisaedados/estudos/estudo-internet-das-coisas-iot/estudo-internet-das-coisas-um-plano-de-acao-para-o-brasil

[272] BANCO NACIONAL DE DESENVOLVIMENTO ECONÔMICO E SOCIAL (BNDES). Produto 7B: Aprofundamento de Verticais – Saúde. 2017. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinternetdascoisas/fase3_7b_relatorio-de-aprofundamento-das-verticais-saude.pdf

externas), o envelhecimento da população, a sustentabilidade financeira, e a satisfação dos cidadãos e profissionais. A "inflação médica", impulsionada pela incorporação de novas tecnologias e pelo envelhecimento da população, ameaça a sustentabilidade do sistema. Apesar dos gastos significativos, os resultados em Saúde no Brasil ainda ficam abaixo de outros países com níveis de investimento semelhantes.

- Potencial da IoT: A IoT pode desempenhar um papel crucial na superação desses desafios, com aplicações em áreas como tratamento de doenças crônicas, controle de doenças infectocontagiosas, promoção e prevenção da Saúde, e melhoria na gestão. O Relatório destaca exemplos de aplicações de alto impacto, como o monitoramento remoto de pacientes com diabetes, a localização de ativos em unidades de Saúde, o apoio ao diagnóstico de sepse, o diagnóstico descentralizado e a identificação e controle de epidemias.
- Competências Tecnológicas: O desenvolvimento e a adoção da IoT em Saúde requerem competências tecnológicas em áreas como dispositivos (sensores, armazenamento de energia, sistemas embarcados), conectividade (redes de curto alcance, redes LPWA), suporte à aplicação (*analytics, middleware* IoT), e segurança da informação (criptografia, *blockchain*). O relatório apresenta uma análise das necessidades tecnológicas e da capacidade do Brasil em cada área, identificando áreas de maior e menor expertise.

18. O Estudo, portanto, propõe uma visão de longo prazo para a IoT na Saúde, com o objetivo de ampliar o acesso à Saúde de qualidade através de uma visão integrada dos pacientes, descentralização da atenção, estímulo ao desenvolvimento da tecnologia e maior eficiência das unidades de Saúde. Essa visão é baseada em experiências internacionais, nas diretrizes do Conselho Nacional de Saúde e nos objetivos do Plano Nacional de Saúde. O Relatório também destaca ainda as barreiras que impedem a concretização dessa visão, como a falta de capital humano especializado, a burocracia para obtenção de recursos e a falta de conectividade em áreas remotas.

Plano Brasileiro de Inteligência Artificial (PBIA)

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

19. O PBIA, conhecido como "Plano de IA para o Bem de Todos"[273], elaborado Ministério da Ciência, Tecnologia e Inovação – MCTI[274] - a pedido do Presidente da República, é estruturado em suas Ações de Impacto Imediato e Ações Estruturantes, prevê diversas iniciativas e investimentos na área da Saúde, com foco na melhoria dos serviços públicos e na promoção do bem-estar social através da Inteligência Artificial. O Plano identifica a Saúde como uma das áreas prioritárias para a aplicação da IA, com o objetivo de aprimorar a eficiência, a qualidade e o acesso aos serviços de Saúde no Brasil, particularmente no âmbito do Sistema Único de Saúde (SUS), o PBIA estabelece:

E.1. Ações de Impacto Imediato na Saúde:

- Projeta o desenvolvimento e implementação de 31 ações de impacto imediato na área da Saúde, divididas em duas categorias: "Saúde no SUS" e "Saúde - Demais Instituições";
- Destaca sete iniciativas "Saúde no SUS" que visam a otimização de processos, diagnósticos e gestão dentro do sistema público de Saúde;
- Prevê cinco iniciativas "Saúde – Demais Instituições", incluindo projetos como a desinfecção autônoma de ambientes, o uso de IA e Big Data para tratamento de câncer, e a prevenção de AVC e Cardiopatia em clientes de Saúde suplementar;
- Estabelece a ação de "IA nos Hospitais da EBSERH/MEC," que visa utilizar IA para diagnóstico por imagem em hospitais federais. Esta ação, porém, ainda aguarda a definição da fonte orçamentária.

E.1.1. Iniciativas-chave no âmbito do SUS:

  - Prontuário Falado no SUS: visa automatizar a transcrição de teleconsultas, com o objetivo de melhorar a eficiência na documentação clínica e a qualidade do atendimento;
  - IA para Suporte a Decisões de Compras de Medicamentos no SUS: busca aprimorar o planejamento e a execução das compras governamentais de medicamentos;

[273] BRASIL. Ministério da Ciência, Tecnologia e Inovação. Inteligência Artificial para o Bem de Todos: Proposta de Plano Brasileiro de Inteligência Artificial 2024-2028. 29 jul. 2024. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/cct/legislacao/arquivos/IA_para_o_Bem_de_Todos.pdf.

[274] A Proposta do Plano Brasileiro de Inteligência Artificial (PBIA) foi aprovada em reunião Plenária no Conselho Nacional de Ciência e Tecnologia – CCT em 29 de julho de 2024, e será encaminhado para o Presidente da República.
BRASIL. Ministério da Ciência, Tecnologia e Inovação (MCTI). Resolução nº 4, de 8 de novembro de 2024. Publicada em: 12 nov. 2024. Disponível em: https://www.in.gov.br/web/dou/-/resolucao-n-4-de-8-de-novembro-de-2024-595418946.

- Otimização dos Diagnósticos no SUS: visa aumentar a precisão e a agilidade nos diagnósticos médicos, especialmente em condições críticas;
- IA em Saúde Bucal no SUS: tem como objetivo melhorar a qualidade dos serviços de Saúde bucal e o prognóstico de câncer oral;
- IA para Detecção de Anomalias nos Procedimentos Hospitalares e Ambulatoriais no SUS: visa identificar padrões anormais em faturamentos e procedimentos, prevenindo irregularidades;
- Idoso Bem Cuidado no SUS: consiste em uma plataforma de IA para promoção e cuidado da Saúde do idoso, com foco no diagnóstico precoce de doenças neurodegenerativas;
- IA para Suporte à Gestão de Processos de Judicialização no SUS: visa aprimorar a gestão de processos de judicialização na Saúde.

E.2. Ações Estruturantes. Eixo 3: IA para Melhoria dos Serviços Públicos

20. Dentre as Ações Estruturantes do PBIA, o Eixo 3 elenca inúmeras iniciativas de IA voltadas para a prestação de serviços públicos de forma mais eficiente. Prevê a destinação de R$ 1,76 bilhão para 19 ações, incluindo a criação de uma infraestrutura nacional de dados, o que também afetará a melhoria da Saúde no país. Dentre as propostas que envolvem o tratamento de dados pessoais e, indiretamente, o setor de Saúde, merecem destaque:

- **Personalização dos Serviços Públicos:** cujo desafio é ampliar a oferta de conteúdo dos diversos órgãos e entidades públicas federais para os cidadãos de maneira personalizada e proativa;
- **Privacidade e Segurança da Informação no Setor Público**: um conjunto de ações abrangentes de privacidade e segurança da informação nos órgãos federais que buscará garantir a privacidade e a segurança das informações dos cidadãos na prestação dos serviços públicos.

21. Como se percebe, a digitalização do setor vem transformando a prestação dos serviços de Saúde, tornando-os mais acessíveis e eficientes, proporcionando melhora da qualidade de vida de milhares de pessoas. As diversas políticas públicas nacionais mencionadas acima, que trazem planos para o país, demonstram essa relevância e estimulam iniciativas que buscam integrar Saúde digital, pesquisa científica e novas tecnologias como pilares para impulsionar a competitividade e modernização do setor.

22. Harmonizar essas estratégias governamentais é crucial para assegurar a segurança, a ética e a transparência no tratamento lícito e responsável dos dados pessoais, fortalecendo, assim, a confiança da população e das

instituições no avanço da Saúde digital. Esse alinhamento não só protege os direitos de liberdade e a vida dos indivíduos, mas também promove equilíbrio entre inovação, sustentabilidade e conformidade legal em um setor que é estruturante para o desenvolvimento econômico do Brasil.

2.1. O tratamento de dados pessoais como fator condicionante para a prestação de serviços de Saúde

23. O tratamento de dados pessoais é essencial para os avanços pretendidos. Nesse sentido, podemos citar alguns exemplos de atividades que dependem, em algum nível, do tratamento de dados pessoais ou que podem, por meio deles, ser significativamente otimizadas:

I. Identificação do Usuário e Registro de Documentos: dados pessoais são utilizados principalmente para a emissão de documentos como Resultado de Exame, Carteira Nacional de Vacinação e Certificado de Vacinação Covid-19, manutenção de credenciais em sistemas e envio de notificações relacionadas a atendimentos e exames;

II. Personalização da Experiência do Usuário: a coleta de dados tem como objetivo melhorar e personalizar a experiência de uso dos aplicativos e sistemas de Saúde. Informações como a localização do usuário, quando fornecida, permite a recomendação de serviços de Saúde em localidades próximas;

III. Dados de Saúde e Histórico Médico: o tratamento de dados como alergias, histórico de IMC, pressão arterial, glicose, doações de sangue, e vacinas administradas tem como finalidade melhorar o atendimento e a personalização dos serviços. Esses dados são frequentemente registrados pelo próprio usuário, que pode manter um histórico atualizado e acessível, além de permitir a comunicação eficiente com profissionais de Saúde e a gestão de tratamentos médicos;

IV. Gestão de Vacinação e Exames Médicos: dados são coletados diretamente de sistemas de Saúde pública para fins de controle e certificação de vacinação, como também para proporcionar fácil acesso aos usuários e permitir o acompanhamento médico eficiente e possibilitar a integração com outros serviços de Saúde e informações públicas;

V. Contatos de Emergência e Profissionais de Saúde: informações utilizadas para garantir que, em situações críticas, o usuário possa ser rapidamente assistido ou comunicado, contribuindo para a eficiência e segurança dos atendimentos médicos.

VI. Serviços e Programas de Saúde Pública: instituições de Saúde também tratam dados relacionados a medicamentos dispensados, como os programas Farmácia Popular e Sistema Horus, para gerenciar a entrega de medicamentos aos usuários e tratam dados cadastrais para lista de espera para transplantes de órgãos e tecidos para ajudar na gestão do Sistema Nacional de Transplantes;

VII. Atividades Hospitalares e Procedimentos Médicos: dados são tratados para agendamento de atendimentos, incluindo atendimentos domiciliares, é essencial para garantir que os usuários possam ser atendidos de acordo com sua disponibilidade e necessidades. Além disso, são usados para a criação de prontuários médicos nas unidades de Saúde, o que assegura o registro completo e atualizado do histórico de Saúde do paciente;

VIII. Comunicação com a Central de Atendimento e Envio de Comunicações: traz eficiência à interação com usuários que são informados sobre agendamentos, resultados de exames, mudanças nos serviços e outras atualizações relevantes;

IX. Doações e Projetos Institucionais: dados pessoais também podem ser utilizados, de maneira consentida, para doações voltadas aos projetos sociais e outras iniciativas das instituições de Saúde;

X. Estudos e Pesquisas Clínicas: esses dados para pesquisas clínicas são essenciais para o avanço da medicina, permitindo que as instituições conduzam estudos de impacto e melhorias nos tratamentos e na prevenção de doenças;

XI. Gestão de Pagamentos e Cobranças: dados financeiros, ou informações bancárias, podem ser utilizados para seguir com pagamentos relativos a serviços de Saúde prestados pela instituição, facilitando a realização de transações financeiras de forma segura e transparente;

24. Dentro desse cenário, há diversas iniciativas em curso no Setor Público que já buscam extrair as melhores vantagens das tecnologias que envolvem o tratamento de dados pessoais para elevar o nível dos serviços prestados pelo Sistema Único de Saúde (SUS), a saber:

XII. O Meu SUS Digital: aplicativo oficial do Ministério da Saúde, desenvolvido para permitir que o cidadão acesse e acompanhe seu histórico clínico de maneira prática e eficiente, por meio de informações SUS;

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

XIII. A Rede Nacional de Dados em Saúde (RNDS): plataforma nacional voltada para a integração e interoperabilidade de informações no setor de Saúde. Implementada desde 2019 no Brasil, no contexto das iniciativas de transformação digital da Saúde, seu principal objetivo é servir como ferramenta para entidades públicas e privadas do setor;

XIV. Prontuário Falado no SUS: por meio do uso de inteligência artificial (IA), é usado para automatizar a transcrição das teleconsultas realizadas no Sistema Único de Saúde (SUS). Durante as consultas remotas, a IA captura e processa as informações faladas pelos profissionais de Saúde e pacientes, convertendo-as em texto de forma precisa e rápida, melhorando, assim, a qualidade do atendimento e a organização dos registros médicos;

XV. Otimização dos Diagnósticos no SUS: utiliza um sistema de inteligência artificial (IA) para melhorar a precisão e a agilidade dos diagnósticos médicos, especialmente em condições críticas e doenças graves como AVC, pneumonia, câncer de mama, tuberculose e melanoma, entre outras. Com isso, a aplicação da IA no diagnóstico médico no SUS busca acelerar o processo de decisão e proporcionar um atendimento mais eficiente, principalmente em situações de urgência;

XVI. Idoso Bem Cuidado no SUS: usa uma plataforma de inteligência artificial (IA) para promover e cuidar da Saúde dos idosos, com foco no diagnóstico precoce de doenças neurodegenerativas, como a doença de Alzheimer, a doença de Parkinson e outras demências;

XVII. IA Generativa para Personalização no Cuidado da Saúde: se vale de um assistente de inteligência artificial (IA) para otimizar a personalização do cuidado em Saúde, com foco na Atenção Primária à Saúde Digital, adaptando os tratamentos e cuidados médicos às necessidades específicas de cada paciente. O grande desafio dessa iniciativa é tornar a medicina personalizada acessível em larga escala, permitindo que um número significativo de pessoas se beneficie de cuidados de Saúde adaptados às suas condições e necessidades específicas;

XVIII. Repositório COVID-19 *Data Sharing*/BR: uma iniciativa da FAPESP em parceria com a Universidade de São Paulo (USP) e, inicialmente, com a colaboração do Instituto Fleury, Hospital Sírio-Libanês e Hospital Israelita Albert Einstein. O principal objetivo desse repositório é disponibilizar dados relacionados à COVID-19 para auxiliar em pesquisas científicas sobre a pandemia. Vale ressaltar que os dados

atualizados periodicamente, além de serem pseudonimizados pelas instituições de Saúde participantes[275];

XIX. Câmara da Saúde 4.0[276]: lançada em 2020, é um fórum coordenado pelo Ministério da Saúde (MS) e da Ciência, Tecnologia e Inovações (MCTI), com participação de instituições públicas e privadas empresariais, governamentais e acadêmicas[277]. Seu objetivo é implementar ações destinadas à melhoria da efetividade da assistência à Saúde por meio do monitoramento contínuo dos pacientes e da adoção de soluções de Internet das Coisas (IoT); promover soluções desenvolvidas localmente para desafios da Saúde com uma visão centrada no paciente; promover a conectividade visando à integração do Sistema Único de Saúde;

XX. Rede Universitária de Telemedicina (RUTE)[278]: iniciativa do Ministério da Ciência e Tecnologia, apoiada pela Financiadora de Estudos e Projetos (Finep) e pela Associação Brasileira de Hospitais Universitários (Abrahue) e coordenada pela Rede Nacional de Ensino e Pesquisa (RNP), que busca aprimorar projetos de telemedicina existentes e incentivar novos trabalhos interinstitucionais.

2.2. Principais Riscos Associados ao Tratamento de Dados Pessoais na Saúde

25. O estudo antes mencionado do BNDES e do MCTI[279] aborda os principais riscos relacionados à privacidade e proteção de dados dos indivíduos no setor da Saúde e destaca a necessidade de regulamentação, alinhamento entre legislações existentes e fiscalização robusta para garantir que o tratamento desses dados pessoais sensíveis ocorra de forma condizente com a legislação. Muitos desses riscos já foram endereçados pela LGPD, pela regulamentação da Lei produzida pela ANPD e pela legislação setorial. De todo modo, abaixo foram os pontos destacados:

---

[275] FUNDAÇÃO DE AMPARO À PESQUISA DO ESTADO DE SÃO PAULO (FAPESP). Repositório *Data Sharing.* Disponível em: https://repositoriodatasharingfapesp.uspdigital.usp.br/.
[276] BRASIL. Ministério da Ciência, Tecnologia e Inovação (MCTI). Câmara Brasileira de Saúde 4.0. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/camara-saude.
[277] Vide Acordo de Cooperação Técnica (ACT) entre MCTI e Ministério da Saúde. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivoscamarasaude/cs-act-mctic-saude.pdf.
[278] REDE NACIONAL DE ENSINO E PESQUISA (RNP). Rede Universitária de Telemedicina (RUTE). Disponível em: https://rcc.rnp.br/RUTE.
[279] BNDES, 2017.

- Complexidade do ecossistema digital na Saúde: a transformação digital no setor intensificou a circulação de dados sensíveis, com um ecossistema labiríntico que envolve desde agentes regulados até atores externos, como *big techs e healthtechs*, muitos sem licenças sanitárias. Essa estrutura demanda maior regulamentação e supervisão para evitar abusos e garantir a conformidade com a LGPD;

- Dados sensíveis como alvo de ataques: dados de Saúde possuem alta criticidade e valor no mercado ilegal (*dark web*), o que os torna alvos frequentes de ciberataques. A interoperabilidade e o uso intensivo desses dados por APIs, dispositivos vestíveis e plataformas digitais aumentam os riscos de vazamento e uso indevido;

- Deficiências regulatórias da ANPD: a ausência de uma abordagem específica para a Saúde na Agenda Regulatória da ANPD contribui para lacunas na interpretação e aplicação da LGPD no setor. Há também desafios relacionados à definição precisa das categorias de dados sensíveis e à aplicação de bases legais adequadas, como o uso indiscriminado da hipótese de "tutela da Saúde" para finalidades inadequadas;

- Potencial de violação de direitos fundamentais: dados pessoais tratados fora das hipóteses legais adequadas podem gerar discriminações ilícitas e preconceitos, especialmente em cenários que envolvem dados genéticos, biométricos e sobre condições de Saúde;

- Uso emergente de tecnologias disruptivas: soluções tecnológicas avançadas, como *blockchain* e neurotecnologia, oferecem benefícios, mas também introduzem riscos únicos, como o tratamento de dados neurais. É essencial que a regulamentação aborde esses novos cenários de forma a equilibrar inovação e proteção de dados e da privacidade do indivíduo;

- Alinhamento com novas legislações: a entrada em vigor da Lei 14.874/2024, que dispõe sobre pesquisa com seres humanos e institui o Sistema Nacional de Ética em Pesquisa com Seres Humanos, cria um cenário em que a LGPD possui aplicação subsidiária. Isso exige que a ANPD revise seus estudos técnicos e coordene esforços com outros órgãos, como o Ministério da Saúde, para garantir que os dados tratados em pesquisas estejam devidamente protegidos.

26. Portanto, embora sejam inúmeros os desafios, existem meios adequados para endereçá-los, não apenas pela legislação de proteção de dados (composta, principalmente, pela LGPD e atos normativos da ANPD, além

dos inúmeros normativos setoriais) que vem a cada dia se consolidando, mas também pelas práticas que os agentes de tratamento vêm adotando, e cooperações nacionais e internacionais para o cumprimento da legislação de proteção de dados.

27.Portanto, para que não se tenha dúvida sobre a possibilidade de tratamento de dados pessoais para o desenvolvimento do setor da Saúde, a premissa que deve pautar as diretrizes da Política Nacional de Proteção de Dados Pessoais e privacidade nesse setor, é que a LGPD não veio proibir o tratamento de dados pessoais nesse contexto, mas sim fornecer meios para que o tratamento de dados pessoais seja feito de forma segura, lícita e responsável, de modo que diretrizes claras, fiscalização efetiva e a criação de um ambiente jurídico que promova tanto a inovação quanto a segurança e privacidade são essenciais para a prosperidade desse setor.

3. CONFORMIDADE LEGAL E USO ÉTICO DOS DADOS PESSOAIS, NO BRASIL E EM OUTRAS JURISDIÇÕES

3.1. Abordagens Regulatórias Associadas à Área da Saúde

28. A Saúde é um setor amplamente regulado no Brasil, havendo destaque, com relação à proteção de dados pessoais, para a LGPD. Contudo, outras leis são aplicáveis exigindo o tratamento ético e adequado dos dados relacionados a esse setor. Vejamos:

Lei Geral de Proteção de Dados Pessoais (“LGPD”)

29. No setor da Saúde, a Lei Geral de Proteção de Dados Pessoais (LGPD) oferece um marco importante para garantir que o tratamento de dados pessoais seja realizado de forma ética, segura e responsável, especialmente considerando a natureza sensível das informações tratadas. A aplicação de medidas legais mais rigorosas são proporcionais aos riscos do tratamento, uma vez há um maior potencial de impacto negativo em caso de uso incorreto ou ilícito desses dados.

30. Nesse sentido, a Lei exige que o tratamento respeite, dentre outros, os princípios da finalidade, da necessidade, adequação e minimização de dados, ou seja, apenas os dados indispensáveis devem ser coletados

e usados e de maneira coerente com a finalidade. Os princípios da não discriminação, da prevenção e da segurança também se destacam no contexto da Saúde, cabendo ao agente de tratamento adotar medidas técnicas e organizacionais de segurança para prevenir acessos não autorizados, perdas, vazamentos ou qualquer outra forma de tratamento indevido dos dados.

31. No que tange às bases legais para o tratamento de dados pessoais sensíveis, a LGPD as trata de forma diferenciada e estão previstas no seu artigo 11.

32. No caso específico de dados de saúde, há outros dispositivos específicos como a vedação (i) da comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxiliares de diagnose e terapia, salvo exceções expressamente previstas[280]; (ii) do tratamento de dados de saúde para prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários das operadoras de planos privados de assistência à saúde[281]. Ademais, no âmbito de estudos em saúde pública, a LGPD determina que (iii) os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas[282].

33. A LGPD ainda incentiva a adoção de boas práticas e governança, como a implementação de políticas de *compliance* e exige a nomeação de um encarregado pelo controlador para supervisionar o cumprimento da legislação. Essas diretrizes e obrigações legais reforçam a proteção dos dados sensíveis e garantem o equilíbrio entre inovação tecnológica e o respeito à privacidade dos indivíduos.

34. Além da LGPD, abaixo estão algumas das principais normas mais abrangentes que compõem o marco regulatório da saúde no país:

[280] V. Artigo 11 §4º da LGPD. O compartilhamento somente é permitido se em benefício do titular de dados e para permitir: (I) I- a portabilidade de dados quando solicitada pelo titular; ou (II) as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo.
[281] V. Artigo 11 §5º da LGPD.
[282] V. Artigo 13 e seus §§ da LGPD.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

Lei 8.080/1990 (Lei Orgânica da Saúde)

- Define as bases do Sistema Único de Saúde (SUS), instituindo os princípios da universalidade, integralidade, descentralização e participação da comunidade.
- Estabelece as diretrizes para a organização, a prestação e a regulamentação dos serviços de saúde no Brasil.

Lei 8.142/1990

- Regula a participação da comunidade e o controle social no SUS, determinando a criação de conselhos de saúde em todas as esferas para fiscalizar e deliberar sobre políticas públicas de saúde.

Código de Ética Médica (Resolução CFM nº 2.217/2018)

- Regulamenta o exercício da profissão médica e os deveres dos profissionais, com foco na ética, confidencialidade e respeito ao paciente.

Lei 9.656/1998

- Regula os planos e seguros privados de assistência à saúde, estabelecendo normas sobre contratação, funcionamento e fiscalização desses serviços.

Normas da Agência Nacional de Saúde Suplementar (ANS)

- Regulamenta os planos de saúde, garantindo os direitos dos usuários, estabelecendo normas de cobertura mínima, e fiscalizando as operadoras de planos de saúde.

Lei 14.874/2024

- Regula a realização de pesquisas envolvendo seres humanos, estabelecendo diretrizes para o consentimento livre e esclarecido e a proteção dos direitos dos participantes em estudos científicos.

Lei 14.510/2022

- Altera a Lei Orgânica da Saúde para definir a telessaúde, modalidade de prestação de serviços de saúde a distância, por meio da utilização das tecnologias da informação e da comunicação, que envolve, entre outros, a transmissão segura de dados e informações de saúde, por meio de textos, de sons, de imagens ou outras formas adequadas.

Normas da Agência Nacional de Vigilância Sanitária (ANVISA)

- Regula a vigilância sanitária, o controle e a fiscalização de produtos e serviços de saúde, como medicamentos, dispositivos médicos, equipamentos e produtos para diagnóstico.

35. Essas são algumas das normas que, junto com a LGPD, formam o arcabouço jurídico que rege a saúde no Brasil, garantindo a proteção dos direitos dos indivíduos e o funcionamento do sistema de saúde.

Regulamento Geral de Proteção de Dados (GDPR)

36. Na mesma linha da LGPD, o GDPR, aplicável no Espaço Econômico Europeu, em sua abordagem sobre dados pessoais, reconhece a importância de um tratamento cuidadoso das categorias de dados, chamadas de "especiais", como os dados de Saúde, devido à sua maior sensibilidade e estabelece um controle maior em seu tratamento.

37. Assim, o GDPR estabelece que esses dados devem ser tratados em alguns contextos específicos, ou seja, desde que necessários (i) para fins de medicina preventiva ou ocupacional, para a avaliação da capacidade de trabalho do empregado, diagnóstico médico, fornecimento de cuidados de saúde ou sociais, tratamento, ou gestão de sistemas e serviços de saúde ou sociais com base na legislação da União ou dos Estados-Membros, ou em contrato com profissional de saúde, sob as condições e salvaguardas estabelecidas em lei[283]; (ii) por razões de interesse público na área da saúde pública, como a proteção contra sérias ameaças transfronteiriças à saúde ou a garantia de elevados padrões de qualidade e segurança dos cuidados de saúde e dos produtos ou dispositivos médicos, com base na legislação da União ou dos Estados-Membros, que preveja medidas adequadas e específicas para salvaguardar os direitos e liberdades do titular dos dados, em particular o sigilo profissional.

[283] V. Artigo 9º (2) (h) (i) do GDPR.

38. O GDPR também incentiva a inovação ao equilibrar a necessidade de proteção com a promoção de um fluxo livre de dados pessoais dentro da União Europeia.

Regulamento de Dispositivos Médicos (MDR) da União Europeia

39. O *Medical Device Regulation*, que entrou em vigor em maio de 2021 no âmbito da União Europeia, representa um avanço significativo para a segurança jurídica e a inovação no setor de Saúde. Ao estabelecer um conjunto claro de normas para a regulamentação de dispositivos médicos, o MDR garante maior transparência e confiabilidade, o que cria um ambiente propício para a inovação. Requisitos como a publicação de resumos de segurança e desempenho clínico para dispositivos de alto risco, a utilização de identificadores exclusivos (UDI) para cada dispositivo e a exigência de coleta de dados pós-comercialização asseguram não apenas a proteção dos pacientes, mas também um processo regulatório robusto que inspira confiança nos novos produtos e tecnologias. Esse marco regulatório facilita a introdução de inovações, pois estabelece uma base sólida de segurança jurídica, permitindo que fabricantes e pesquisadores possam desenvolver soluções mais eficazes com maior clareza e previsibilidade.

HIPAA

40. O *Health Insurance Portability and Accountability Act* (HIPAA), de 1996, uma lei nacional dos Estados Unidos. O HIPPA visa proteger a privacidade das informações de Saúde identificáveis dos indivíduos e estabelece padrões nacionais para o uso e a divulgação desses dados por entidades cobertas, como provedores de Saúde, seguradoras e outras instituições.

Supervisão e Aplicação da Lei

Reino Unido:

41. O *Information Commissioner's Office* (ICO), autoridade de dados do Reino Unido, disponibiliza um **guia detalhado sobre o tratamento de dados de Saúde**[284], abordando aspectos como segurança, direito de acesso,

[284] *INFORMATION COMMISSIONER'S OFFICE (ICO). Right of Access: Health Data*. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/health-data/.

restrições e obrigações das organizações. O documento orienta sobre como responder a solicitações de acesso (SARs) de maneira adequada, incluindo exceções quando a divulgação pode causar danos graves à Saúde mental ou física de qualquer pessoa. O guia também aborda o compartilhamento de dados com terceiros, estabelecendo limites claros para proteger os direitos dos titulares, especialmente no caso de informações sensíveis. As orientações do ICO reforçam a importância de medidas rigorosas de segurança e transparência, garantindo que organizações na área da Saúde cumpram suas obrigações legais enquanto protegem dados sensíveis. Essa abordagem consultiva promove maior confiança entre cidadãos e entidades de Saúde, além de mitigar riscos legais e fortalecer as práticas de governança no setor.

União Europeia:

42. Em 2020, o EDPB publicou diretrizes voltadas ao tratamento de dados de Saúde em pesquisas científicas no contexto da pandemia de COVID-19[285]. Reconhecendo a urgência de medidas globais, o EDPB esclareceu que o GDPR não impede o uso de dados para pesquisas médicas, mas estabelece salvaguardas rigorosas para proteger os direitos fundamentais dos titulares. O documento reforçou que o uso secundário de dados, como a reutilização de informações coletadas para outros fins, deve seguir o princípio de compatibilidade de propósitos e ser acompanhado de medidas técnicas e organizacionais robustas. De mais a mais, o EDPB destacou a importância de avaliações de impacto à proteção de dados (DPIA) para identificar e mitigar riscos associados ao tratamento de dados no contexto emergencial.

43. Em 2021, o EDPB ampliou as orientações para o uso de dados de Saúde em pesquisas científicas, além do contexto da pandemia, oferecendo diretrizes mais abrangentes[286]. O Comitê reforçou a necessidade de garantir que o tratamento de dados sensíveis respeite os princípios do GDPR, como limitação de finalidade e minimização de dados. Também enfatizou a importância da transparência, com informações claras aos titulares, especialmente no caso de tratamentos que envolvam finalidades secundárias, armazenamento e descarte dos dados. Outro foco das diretrizes foi a harmonização das legislações nacionais para reduzir divergências que

[285] *EUROPEAN DATA PROTECTION BOARD (EDPB). Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak*. 2020. Disponível em: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf.

[286] *EUROPEAN DATA PROTECTION BOARD (EDPB). EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research.* 02 fev. 2021. Disponível em: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_replyec_questionnaireresearch_final.pdf.

possam dificultar projetos transfronteiriços de pesquisa. O EDPB recomendou salvaguardas adicionais, como pseudonimização, criptografia e limites rigorosos de acesso, para proteger os direitos dos titulares.

Cooperação Internacional:

44. As Autoridades de Proteção de Dados igualmente desempenham um papel essencial na cooperação com autoridades de dados estrangeiras, participando de fóruns e comitês internacionais, como o Comité Europeu para a Proteção de Dados (CEPD), colaborando para a harmonização das práticas de proteção de dados em diferentes jurisdições.

Iniciativa Relevante Na União Europeia: Espaço Europeu de Dados de Saúde (EEDS)[287]

45. O EEDS é uma proposta da Comissão Europeia que visa criar uma infraestrutura robusta para o compartilhamento seguro e ético de dados de Saúde eletrônicos. A iniciativa busca não apenas facilitar a criação de uma União Europeia da Saúde, mas também maximizar os benefícios do intercâmbio, uso e reuso de dados de saúde, promovendo avanços na pesquisa médica, na inovação e na segurança dos cuidados de saúde.

46. Um dos pilares do EEDS é o fortalecimento do controle dos indivíduos sobre seus dados pessoais de saúde pessoais, assegurando transparência e proteção contra seu uso ilícito ou inadequado. Nele estão incluídos mecanismos para que os indivíduos possam acessar e gerenciar seus dados, além de garantir que o tratamento secundário de dados respeite finalidades claras e proporcione benefícios à saúde pública e à segurança social. Seguem os benefícios e desafios identificados:

- Aproveitamento de Dados Sensíveis para o Interesse Público: a proposta prevê o uso secundário de dados de Saúde eletrônicos em pesquisas e políticas de Saúde pública, desde que devidamente regulado. Isso pode acelerar descobertas médicas e aprimorar os sistemas de Saúde;

- Infraestrutura e Supervisão Eficaz: para suportar o grande volume de dados sensíveis, o EEDS propõe uma infraestrutura tecnológica avançada e um modelo de governança que delimite claramente as

[287] *EUROPEAN DATA PROTECTION BOARD (EDPB).* O Espaço Europeu de Dados de Saúde deve assegurar uma forte proteção dos dados de saúde eletrônicos. 14 jul. 2022. Disponível em: https://www.edpb.europa.eu/news/news/2022/european-health-data-space-must-ensure-strong-protection-electronic-health-data_pt?utm_source=chatgpt.com

funções das autoridades envolvidas. Essa governança integrada evita sobreposições de competência e assegura que as autoridades de proteção de dados sejam as principais responsáveis por questões relacionadas à privacidade e segurança;

- Armazenamento de Dados no Espaço Econômico Europeu (EEE): um dos pontos cruciais é garantir que os dados de Saúde permaneçam armazenados no EEE, salvo transferências específicas em conformidade com as disposições do RGPD, minimizando riscos de acesso ilegal ou inadequado;

- Limitação de Finalidades e Transparência: a proposta destaca a necessidade de restringir claramente as finalidades do uso secundário de dados, priorizando casos com impacto direto na Saúde pública e segurança social, alinhando-se às melhores práticas de proteção de dados.

47. Lições para Políticas de Governança: o EEDS demonstra como uma estrutura bem delineada e uma governança integrada pode equilibrar o uso inovador de dados sensíveis com a proteção dos direitos individuais. Também destaca a importância de uma supervisão independente e da coordenação entre as autoridades de proteção de dados, eliminando lacunas regulatórias e promovendo confiança entre indivíduos e organizações. Este modelo oferece um exemplo de como a governança de dados pode ser aprimorada em setores sensíveis como a saúde, fomentando inovação enquanto protege direitos fundamentais.

3.2. Casos Relevantes de Fiscalização da Área da Saúde

48. No âmbito nacional:

- Secretaria de Estado da Saúde de Santa Catarina (SES/SC)[288]: Em 2023, a SES/SC foi alvo de uma fiscalização pela ANPD após um incidente de segurança envolvendo o vazamento de 4 GB de dados sensíveis relacionados ao sistema de regulação hospitalar do SUS, impactando cerca de 48 mil titulares. Apesar da comunicação à ANPD sobre o ocorrido, a Secretaria não conseguiu cumprir os prazos e requisitos previstos na LGPD, incluindo a elaboração de um Relatório de Impacto à Proteção de Dados (RIPD) e a comunicação direta aos titulares afetados. Entre as falhas constatadas, a ANPD destacou a

[288] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Coordenação-Geral de Fiscalização – Coordenação de Fiscalização (FIS/GGF). Relatório de Instrução nº 4/2023/FIS/CGF/ANPD: Processo nº 00261.001886/2022-51.2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/ri-sesc-sc-00261001886202251-autos-publicos.pdf.

inadequação do sistema utilizado, que não atendia aos padrões de segurança exigidos, e a demora na comunicação do incidente. Como consequência, a ANPD aplicou sanções administrativas e determinou medidas corretivas, como a necessidade de comunicação direta aos titulares e melhorias nos mecanismos de segurança da informação.

- Instituto de Assistência Médica ao Servidor Público Estadual de São Paulo (IAMSPE)[289]: Em 2022, o IAMSPE foi autuado pela ANPD por falhas graves em seus sistemas que expuseram dados sensíveis de mais de 1,4 milhão de beneficiários, incluindo informações pessoais e financeiras. O incidente, agravado pelo atraso na comunicação à ANPD e aos titulares, revelou a ausência de medidas de segurança adequadas, como autenticação robusta e rastreamento de acessos. A ANPD aplicou sanções e exigiu medidas para prevenir novos incidentes. Após a autuação, o IAMSPE adotou ações corretivas, como melhorias nos sistemas e treinamentos, mas somente após o ocorrido.

- Ministério da Saúde – Incidente de segurança[290]: Em 2024, a ANPD concluiu um processo envolvendo um incidente de segurança nos sistemas do Ministério da Saúde, que resultou na exposição de dados sensíveis relacionados à Saúde de milhares de cidadãos brasileiros. A falha permitiu o acesso público não autorizado a dados pessoais, incluindo CPFs e informações sensíveis, devido a vulnerabilidades no sistema DATASUS. A investigação revelou violações dos artigos 48 e 49 da LGPD, como a não utilização de sistemas seguros e o atraso na comunicação do incidente aos titulares. O Ministério foi sancionado com advertências e obrigado a implementar medidas corretivas para prevenir novos incidentes. Este caso reforça os riscos de tratamento inadequado de dados em sistemas de Saúde e a necessidade de conformidade com os princípios da LGPD.

[289] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Coordenação-Geral de Fiscalização – Coordenação de Fiscalização (FIS/GGF). Relatório de Instrução n° 2/2023/CGF/ANPD: Processo nº 00261.001969/2022-41. 2023. Disponível em:www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_4286376_relatorio_2_2023.pdf .

[290] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Coordenação-Geral de Fiscalização – Coordenação de Fiscalização (FIS/GGF). Relatório de Instrução nº 4/2024/FIS/CGF/ANPD: Processo nº 00261.001882/2022-73. 2024. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/relatorio_de_instrucao_no_4_2024_fis_cgf_anpd_v-publica.pdf.

- **Ministério da Saúde - Indisponibilidade de serviços do ConecteSUS e sistemas de Saúde[291]:** Em 2024, a ANPD concluiu que um ataque cibernético ao ConecteSUS e a outros sistemas do Ministério da Saúde comprometeu dados sensíveis de milhões de brasileiros e deixou indisponíveis serviços essenciais. A investigação revelou a ausência de um encarregado de dados, a falta de Relatórios de Impacto (RIPDs) e o não cumprimento de padrões exigidos pela LGPD.

- **Nota Técnica sobre o tratamento de dados no varejo farmacêutico[292]:** A Nota Técnica da ANPD revelou questões relevantes no setor farmacêutico quanto ao tratamento de dados pessoais, como coleta excessiva de dados sensíveis, políticas de privacidade insuficientes e falta de transparência em programas de fidelização. Práticas como vincular descontos ao fornecimento de dados pessoais e compartilhamento com terceiros sem clareza foram criticadas. A ANPD recomendou ações educativas e materiais orientativos para aumentar a conscientização e promover boas práticas no setor, recomendando maior transparência, governança de segurança e respeito aos direitos dos titulares.

49. Na Europa, análise conduzida pelo escritório *CMS Law*[293] identificou que, em 2023, 26 países emitiram 202 multas no setor de Saúde, totalizando EUR 16,5 milhões. Apesar de um aumento no número de multas (+48 em relação a 2022), o valor total caiu 70%, refletindo uma tendência de redução nas médias das penalidades. A maioria das violações decorreu da ausência de medidas técnicas e organizacionais adequadas (71 multas, EUR 11,6 milhões). A Itália liderou com 23 multas, seguida por Romênia e Espanha. O relatório concluiu alguns pontos relevantes acerca dos casos de fiscalização e aplicação do GDPR no setor da Saúde:

- A maior parte das infrações continua a surgir de deficiências técnicas e organizacionais, especialmente no contexto de ataques cibernéticos e violação de dados.
- Medidas preventivas são fundamentais, mas a falta de ações rápidas e adequadas durante e após os incidentes aumenta a gravidade das violações.

---

[291] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Coordenação-Geral de Fiscalização – Coordenação de Fiscalização (FIS/GGF). Relatório de Instrução nº 5/2024/FIS/CGF/ANPD: Processo nº 00261.000456/2022-12; 2024. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/relatorio_de_instrucao_5_publico_ocultado.pdf.

[292] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Coordenação-Geral de Tecnologia e Pesquisa (CGTP). Nota Técnica nº 4/2023/CGTP/ANPD: Processo nº 00261.000988/2021-79. 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/nota-tecnica-no-4-2023-farmacias_ret-1.pdf.

[293] KRAUS, Michael. GDPR Enforcement Tracker Report: Health Care. CMS LAW, 2023. Disponível em: https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/health-care.

- O tratamento de dados relacionados à Covid-19 ainda gera multas, sublinhando a necessidade de revisar continuamente a justificativa legal para a coleta e uso de dados pessoais.

50. Quanto aos casos analisados pelas Autoridades de Proteção de Dados, destacam-se:

- Irlanda – Ataque de *Ransomware* e Medidas Técnicas Inadequadas[294]: Em 2023, a maior multa no setor de Saúde foi aplicada na Irlanda, totalizando EUR 460.000. O incidente envolveu um ataque de *ransomware* que resultou no acesso, alteração e destruição não autorizada de dados pessoais de cerca de 70.000 indivíduos, dos quais 2.500 foram afetados permanentemente. A Autoridade de Proteção de Dados identificou falhas graves nas Medidas Técnicas e Organizacionais (TOMs), tanto na prevenção quanto na resposta ao ataque. A ausência de documentação adequada do incidente agravou a infração, evidenciando a necessidade de maior robustez nas medidas preventivas e reativas.

- Itália – Falhas de Segurança em Registros de Saúde: Dois casos na Itália destacaram deficiências nas medidas de segurança relacionadas a registros de Saúde eletrônicos e ataques de *ransomware*. O primeiro caso[295] envolveu o acesso não autorizado a dados de pacientes devido à falta de medidas técnicas adequadas. No segundo caso[296], um ataque de *ransomware* impactou mais de 800.000 pacientes, expondo falhas no uso de autenticação frágil (apenas login e senha) e na detecção tardia do incidente. Ambos os casos resultaram em multas de EUR 30.000 cada.

- Lituânia – Direito de Acesso aos Dados[297]: Pela primeira vez, a Lituânia aplicou uma multa GDPR no setor de Saúde. Um hospital foi multado em EUR 8.000 por falhas no atendimento ao direito de acesso do titular. Embora o pedido tenha sido parcialmente atendido, a instituição não ofereceu informações completas sobre a base legal, finalidades e categorias de destinatários dos dados.

[294] *CMS LAW. Enforcement Tracker Case*: ETid-1666. Disponível em: https://etid.link/ETid-1666.
[295] *CMS LAW. Enforcement Tracker Case*: ETid-1828. Disponível em: https://etid.link/ETid-1828.
[296] *CMS LAW. Enforcement Tracker Case:* ETid-2200. Disponível em: https://etid.link/ETid-2200.
[297] CMS LAW. *Enforcement Tracker Case:* ETid-1633. Disponível em: https://www.enforcementtracker.com/ETid-1633

- **França – Dados de Saúde e Uso de *Cookies*[298][299]:** a Em 11 de maio de 2023, a CNIL multou o site DOCTISSIMO em um caso transfronteiriço por diversas violações ao GDPR e à Lei Francesa de Proteção de Dados. Após investigações motivadas por uma denúncia da *PRIVACY INTERNATIONAL*, foram identificadas as seguintes infrações: armazenamento de dados além do necessário; coleta de dados de Saúde sem consentimento válido; ausência de estrutura legal formalizada para operações conjuntas de tratamento com outro controlador; falhas na segurança dos dados pessoais e uso inadequado de *cookies* (Artigo 82 da Lei Francesa "*Loi Informatique et Libertés*"). Como resultado, a CNIL impôs uma multa de EUR 280.000 pelas violações ao GDPR, com a participação de outras autoridades europeias no âmbito do "*one-stop shop*", e outra de EUR 100.000 pelas infrações específicas relacionadas ao uso de *cookies*, totalizando EUR 380.000. O caso destacou a importância da conformidade em tratamentos de dados sensíveis e no uso de rastreadores digitais.

4. PRÁTICAS A SEREM IMPLEMENTADAS PARA MELHORAR A PROTEÇÃO DE DADOS E SEGURANÇA JURÍDICA NO TRATAMENTO DE DADOS PESSOAIS NA SAÚDE

4.1. Boas Práticas de Governança para Mitigação de Riscos e Conformidade Legal

51. O tratamento de dados pessoais no setor de Saúde exige, além do atendimento à legislação pertinente de proteção de dados, a adoção de práticas de conformidade para atendimento de outras leis setoriais aplicáveis, assim como das instruções das agências reguladoras do setor, como a Agência Nacional de Saúde (ANS) e a Agência Nacional de Vigilância Sanitária (ANVISA) que trazem normas específicas e preveem boas práticas e guias para governança ética desses dados. Exemplos de medidas de boas práticas podem ser percebidas nos Código de Boas Práticas da Confederação Nacional de Saúde[300] (CNSaúde) e diversos Guias publicados e pela ANVISA (Agência Nacional de Saúde)[301], a saber:

---

[298] *COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL). Délibération* SAN-2023-006. 11 mai. 2023. Disponível em: https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000047552103..

[299] *COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL). Données de santé et utilisation des cookies: Doctissimo sanctionné par une amende de 380 000 euros*. 17 mai. 2023. Disponível em: https://www.cnil.fr/fr/donnees-de-sante-et-utilisation-des-cookies-doctissimo-sanctionne-par-une-amende-de-380-000-euros.

[300] CONFEDERAÇÃO NACIONAL DE SAÚDE. Código de Boas Práticas. Disponível em: http://cnsaude.org.br/wp-content/uploads/2021/03/Boas-Praticas-Protecao-Dados-Prestadores-Privados-CNSaude_ED_2021.pdf

[301] AGÊNCIA NACIONAL DE VIGILÂNCIA SANITÁRIA (ANVISA). AnvisaLegis: Lista de Guias. Disponível em: https://anvisalegis.datalegis.net/action/ActionDatalegis.php?acao=recuperarTematicasCollapse&cod_modulo=644&cod_menu=9486.

- **Código de Boas Práticas para Prestadores de Serviços Profissionais de Saúde**[302]: é um importante marco em termos de governança e boas práticas, uma vez que representa o primeiro Código de Conduta voltado aos Prestadores de Serviços de Saúde para a aplicação da LGPD. A proposta, além de direcionar hospitais e laboratórios privados sobre as condutas adequadas, busca fomentar a inovação de forma responsável e fortalecer a confiança dos titulares de dados no setor de saúde;

- **Guia nº 33/2020 (v.1),** publicado em 14/04/2020[303], se refere a Validação de Sistemas Computadorizados, que são utilizados na fabricação de insumos e medicamentos, com foco nas Boas Práticas de Fabricação. Esse Guia serve como referência para garantir que os sistemas envolvidos no desenvolvimento de produtos farmacêuticos e dispositivos médicos operem de forma segura e eficiente, mantendo a conformidade com as normas regulatórias e assegurando a proteção dos dados pessoais dos pacientes.

- **Guia nº 38/2020**, publicado em 25/09/2020[304], que trata dos Princípios e Práticas de Cibersegurança em Dispositivos Médicos. O Guia estabelece princípios que ajudam a garantir que a inovação no uso de dispositivos médicos e outras tecnologias não comprometa a segurança das informações pessoais dos pacientes o qual. A colaboração entre fabricantes, prestadores de serviços de Saúde, usuários e a própria ANVISA é essencial para criar um ambiente de confiança, que permita o uso ético e seguro de tecnologias inovadoras no setor, protegendo os dados pessoais e a continuidade da inovação de forma ética.

---

[302] CNSaúde. Disponível em http://cnsaude.org.br/codigo-de-boas-praticas-protecao-de-dados-para-prestadores-privados-de-servicos-em-saude/#:~:text=A%20Confedera%C3%A7%C3%A3o%20Nacional%20de%20Sa%C3%BAde,Prote%C3%A7%C3%A3o%20de%20Dados%20(LGPD).

[303] AGÊNCIA NACIONAL DE VIGILÂNCIA SANITÁRIA (ANVISA). Guia nº 33: Guia para Validação de Sistemas Computadorizados. 26 mar. 2020. Disponível em: https://anvisalegis.datalegis.net/action/ActionDatalegis.php?acao=abrirTextoAto&link=S&tipo=GUI&numeroAto=00000033&seqAto=222&valorAno=2020&orgao=ANVISA/MS&cod_modulo=644&cod_menu=9486

[304] AGÊNCIA NACIONAL DE VIGILÂNCIA SANITÁRIA (ANVISA). Guia nº 38: Guia sobre Princípios e Práticas de Cibersegurança em Dispositivos Médicos. 14 set. 2020. Disponível em: https://anvisalegis.datalegis.net/action/ActionDatalegis.php?acao=abrirTextoAto&link=S&tipo=GUI&numeroAto=00000038&seqAto=222&valorAno=2020&orgao=ANVISA/MS&cod_modulo=644&cod_menu=9486.

52. Há ainda o **Código de Ética Médica**[305]**,** do Conselho Federal de Medicina no Brasil, que, especificamente no tocante ao compartilhamento de informações do prontuário emitiu o Parecer nº 14/2017 sobre o uso do WhatsApp e demais plataformas de comunicação entre médicos, em caráter privativo, justamente considerando a ampla utilização desses meios de comunicação entre médicos.

53. Ademais, o **Código de Boas Práticas para Proteção de Dados para Prestadores Privados em Saúde,** do CFM, estabelece medidas para o tratamento de dados pessoais, dentre eles um protocolo para compartilhamento de dados, inclusive para compartilhamento de dados pelo Whatsapp.[306]

54. Por fim, a **ANPD, no final de 2024 celebrou com a ANS um Acordo de Cooperação Técnica com a ANS**[307], o qual objetiva, sobretudo, promover ações educativas sobre proteção de dados na saúde suplementar. Dentre os potenciais resultados esperados desse acordo, encontram-se a elaboração de estudos e notas técnicas sobre diversos temas de proteção de dados aplicáveis à saúde suplementar (saúde digital, transferência internacional, interoperabilidade, conservação, anonimização, compartilhamento e eliminação de dados na área de saúde), as quais serão utilizadas na construção de medidas educativas visando a "construção do conhecimento e promoção das melhores práticas relacionados à proteção de dados pessoais e à segurança da informação".

4.2. Práticas que podem ser incentivadas para utilização dos sistemas de IA e respeito à legislação de proteção de dados pessoais

55. O reforço da segurança jurídica no tratamento de dados pessoais de Saúde é essencial para garantir a confiança dos indivíduos, promover a inovação e impulsionar o desenvolvimento econômico. Para tanto várias iniciativas podem ser implementadas, incluindo a adoção de códigos de boas práticas, o uso de *Privacy Enhancing Technologies (PETs)* e a realização de treinamentos especializados, a saber:

[305] Disponível em: https://portal.cfm.org.br/images/PDF/cem2019.pdf.
[306] CONSELHO FEDERAL DE MEDICINA (CFM). Código de Ética Médica: Resolução CFM n° 2.217, de 27 de setembro de 2018, modificada pelas Resoluções CFM nº 2.222/2018 e 2.226/2019. Brasília: 2019. http://cnsaude.org.br/wp-content/uploads/2021/03/Boas-Praticas-Protecao-Dados-Prestadores-Privados-CNSaude_ED_2021.pdf.
[307] Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-ans-firmam-acordo-para-aprimorar-protecao-de-dados-na-area-de-saude

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

- A implementação de códigos de boas práticas específicos para o tratamento de dados pessoais é uma maneira eficaz de assegurar que as organizações cumpram as normas de proteção de dados e de privacidade, além de estabelecer diretrizes claras sobre o uso responsável da informação.

- O uso de *Privacy Enhancing Technologies (PETs)* pode contribuir significativamente para a proteção dos dados pessoais, melhorando a segurança e a privacidade sem comprometer a inovação. As principais PETs, que estão sendo aplicadas no setor de Saúde, incluem o aprendizado federado, a computação segura multipartes e *o blockchain*, cada uma com um papel específico no tratamento e proteção dos dados pessoais na área da Saúde, a seguir detalhadas[308]:

- O aprendizado federado permite treinar modelos de IA e ML localmente, sem compartilhar dados brutos entre instituições. No setor da Saúde, essa tecnologia melhora diagnósticos, como em radiologia e oncologia, ao combinar atualizações de modelos de forma centralizada, garantindo a privacidade dos dados dos pacientes e aumentando a precisão dos resultados.

- Computação Segura Multipartes (*Secure Multi-Party Computation*): A computação segura multipartes permite análises colaborativas entre instituições sem expor dados privados, sendo útil em áreas como genômica e estratificação de risco de pacientes. Embora preserve a confidencialidade, exige confiança entre as partes e protocolos rigorosos para prevenir uso indevido dos dados.

- *Blockchain*: embora não seja exclusivamente uma PET, a tecnologia de *blockchain* pode ser usada para proteger a privacidade dos dados na Saúde ao registrar informações de forma descentralizada, imutável e transparente. Essa tecnologia melhora a interoperabilidade dos registros eletrônicos, aumenta a segurança e facilita a integração de dados de diferentes fontes, ajudando a resolver a fragmentação de informações no setor.

Treinamento e Capacitação no Setor

[308] KENNEDY, Shania. *How Architectural Privacy-Enhancing Tools Support Health Analytics. HealthTech Analytics,* 31 ago. 2023. Disponível em: https://www.techtarget.com/healthtechanalytics/feature/How-Architectural-Privacy-Enhancing-Tools-Support-Health-Analytics#:~:text=Privacy%2Denhancing%20technologies%20(PETs),of%20these%20types%20is%20recommended

56. A capacitação dos profissionais de saúde envolvidos no tratamento de dados pessoais é essencial para garantir a conformidade legal e promover a segurança jurídica. Os treinamentos devem ser contínuos e envolver os seguintes aspectos: (i) treinamento em conformidade regulatória; (ii) capacitação em segurança da informação; (iii) educação sobre ética e privacidade; (iv) simulações de incidentes de segurança (como vazamentos de dados ou ataques cibernéticos) para treinar as equipes em respostas rápidas e eficientes, garantindo que todos saibam como agir para mitigar danos.

Auditorias e Monitoramento Contínuo

57. Além das práticas acima, é fundamental realizar auditorias regulares e monitorar continuamente dos sistemas e processos que envolvem o tratamento de dados pessoais, como: (a) auditorias de conformidade; (b) monitoramento de segurança para detectar possíveis falhas de segurança ou vazamentos de dados em tempo real; (c) revisões dos riscos associados ao tratamento de dados pessoais e implementar estratégias para mitigá-los.

58. Há, portanto, diversas práticas ou iniciativas que podem contribuir no tratamento de dados pessoais de Saúde com segurança jurídica, respeitando os direitos e garantias fundamentais, a LGPD e, ao mesmo tempo, estimular o desenvolvimento econômico, tecnológico e a inovação.

Uso de dados abertos de forma condizente com a legislação

59. Além dessas medidas, os dados abertos têm se mostrado ferramenta essencial para aprimorar a tomada de decisões, apoiar a pesquisa, melhorar a documentação de pacientes e impulsionar a detecção precoce de doenças, contribuindo para o avanço da tecnologia e com o desenvolvimento econômico do país.

60. Inclusive, no Dia Mundial da Saúde, organizado pela Organização Mundial da Saúde (OMS), celebra-se a importância de iniciativas que utilizam dados abertos para promover a Saúde global e atender às necessidades dos mais vulneráveis.[309]

[309] *DATA.EUROPA.EU. World Health Day: Open Data Initiatives in Healthcare*. 07 abr. 2023. Disponível em: https://data.europa.eu/en/news-events/news/world-health-day-open-data-initiatives-healthcare.

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

61. Projetos de dados abertos no setor de Saúde podem ser encontrados no portal ***European Data Portal*** (EDP), o qual oferece mais de 7.000 conjuntos de dados relacionados à Saúde. Esses dados cobrem uma ampla gama de tópicos, como poluição do ar, uso de ambulâncias, tabagismo e acidentes. Esses dados têm o objetivo de aumentar a conscientização sobre os diferentes níveis de qualidade do ar e podem ser reutilizados para criar serviços que promovam a Saúde e proteção da população.[310]

62. Outra iniciativa notável é a **Plataforma Global de Dados Individuais de Pacientes (IPD)**[311]. Em 2021, a Organização Mundial da Saúde (OMS) decidiu apoiar a criação de uma plataforma global de acesso público para dados individuais de pacientes (DPI) relacionados à tuberculose (TB), com o objetivo de consolidar diversos conjuntos de dados em um único recurso agrupado, que servirá tanto para orientar diretrizes futuras quanto para fomentar a ciência aberta, promovendo o compartilhamento de informações no futuro.

63. Já na França se destaca o ***Medicatio***, um banco de dados de medicamentos, desenvolvido a partir do ***Use Case Observatory*** (Observatório de Casos de Uso)[312], que está relacionado aos avanços em programas de acesso antecipado (EAPs) a remédios, com destaque para as que simplificaram os a disponibilização de tratamentos inovadores antes da autorização completa de comercialização. Essas propostas têm como objetivo atender necessidades médicas não supridas, especialmente em casos de doenças graves ou raras. Essa iniciativa posiciona a França como líder no acesso antecipado a medicamentos, promovendo o cuidado ao paciente e incentivando inovações farmacêuticas.

64. Os exemplos citados podem ser considerados como iniciativas a serem exploradas em outros países, como no Brasil, já que garantem a ampliação do uso de dados pessoais de Saúde com segurança jurídica, e incentivam a inovação tecnológica no setor através do tratamento responsável de dados pessoais.

---

[310] *DATA.EUROPA.EU. Open Health Data*. 23 jan. 2019. Disponível em: https://data.europa.eu/en/publications/datastories/open-health-data-european-data-portal

[311] GOODALL, R. L.; FABIANE, S. M.; HAKIMAN, A.; CROOK, A. M.; MIRZAYEV, F.; SCHUMACHER, S.; RANGAKA, M. X. *A publicly accessible global data repository – the WHO TB-IPD platform*. *IJTLD Open*, v. 1, n. 4, p. 151-153, 1 abr. 2024. DOI: https://doi.org/10.5588/ijtldopen.24.0131. PMID: https://pubmed.ncbi.nlm.nih.gov/38988407/; PMCID: PMC11231825.

[312] *EUROPEAN PHARMACEUTICAL REVIEW. France ATU Reform: Early Access Possible*. 06 dez. 2022. Disponível em: https://www.europeanpharmaceuticalreview.com/article/177035/france-atu-reform-early-access-possible/

5. CONCLUSÃO

65. O tratamento dos dados de saúde, conforme estabelecido pela LGPD e pela legislação setorial, assegura não apenas a proteção da privacidade dos indivíduos, como também fortalece a confiança e a segurança jurídica necessárias para que o setor de Saúde se desenvolva de forma segura e sustentável. Ao buscar, rigorosamente, observância à lei, com medidas de governança robustas, as organizações públicas e privadas tornam-se preparadas para tratar os dados pessoais de forma adequada, impulsionando avanços na medicina personalizada, proporcionando mais eficiência, mais precisão, e melhor qualidade na prestação dos serviços públicos e privados de saúde, gerando, com isso, o bem-estar dos indivíduos.

66. Nesse sentido, a adoção de boas práticas, como Códigos de Conduta, Tecnologias de Proteção de Privacidade (PETs), treinamento e capacitação do setor, e a realização de auditorias e monitoramento contínuos, especialmente no setor público de saúde, são medidas interessantes de se analisar e implementar.

67. Ademais, a interoperabilidade de dados emerge como um dos pilares centrais para alavancar projetos de políticas públicas como a Saúde Digital 4.0, o Plano Nacional de Inteligência Artificial (projetos referentes à Saúde), por meio do uso amplo, estratégico, interconectado e responsável dos dados. A integração eficaz de informações entre diferentes atores – tanto públicos quanto privados – possibilita análises mais completas, tomadas de decisão baseadas em evidências e a otimização de recursos que não apenas impulsiona a eficiência operacional do setor, mas também fomenta novos investimentos, incentiva a pesquisa científica e gera soluções inovadoras que beneficiam diretamente a sociedade.

68. Assim, o avanço da governança de dados na saúde, liderado por iniciativas como as da ANPD e organizações e órgãos setoriais, pode posicionar o Brasil como referência na construção de um ecossistema de saúde sustentável e tecnologicamente avançado. Essa coordenação e alinhamento entre diversas entidades públicas e iniciativas governamentais existentes precisam ser fortalecidas e são cruciais para garantir práticas éticas e responsáveis no uso desses dados.

69. Tendo em vista a imprescindibilidade do tratamento de dados pessoais nesse contexto, é fundamental que a Política Nacional de Proteção de Dados Pessoais e Privacidade reconheça o setor de Saúde como prioritário e fomente o tratamento desses dados em prol do desenvolvimento e bem-estar das pessoas. Essa chancela

estimulada pela PNPD assegurará o uso seguro, transparente e eficiente dos dados de saúde, fomentando a confiança, a inovação e o desenvolvimento tecnológico do setor.

São Paulo, 22 de janeiro de 2024.

Rony Vainzof
Conselheiro Titular do CNPD.

Conselho Nacional de
Proteção de Dados
Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

ANEXO XXX – PARECER CONCLUSIVO - DIVERGÊNCIA DE VOTO: CONSELHEIRO ALEXANDRE BOAVA

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

GT5
DADOS PESSOAIS PARA O DESENVOLVIMENTO ECONÔMICO, TECNOLÓGICO E A INOVAÇÃO

PARECER CONCLUSIVO- DIVERGÊNCIA DE VOTO

Conselheiro: Alexandre Boava

Itens 6.b, 6.d e 6.e do Parecer Conclusivo

6. Estimular práticas de proteção de dados por meio de incentivos regulatórios e econômicos, beneficiando tanto o setor público quanto o privado, como nos seguintes exemplos:

6.b. 2° Subsídios ou descontos tributários vinculados à certificação em proteção de dados;

Justificativa: Essa prática pode se tornar mais um mecanismo de incentivo fiscal, sobretudo, para grandes empresas que já se beneficiam de outras políticas de incentivo. A proteção de dados é um direito fundamental e não deve ser estimulada via contrapartidas econômicas, outros mecanismos de apoio e responsabilização devem ser estimulados.

6.d. Prioridade em licitações e contratos públicos

Justificativa: Essa prática pode criar um acúmulo de contratos para empresas que já tem em seus processos práticas de proteção de dados por conta dos riscos associados a operação em detrimento de outras que, por serem menores ou não estarem associadas a um alto risco, não tenham práticas sofisticadas em nenhum grau do tratamento de dados pessoais.

6.e. Divulgar anualmente um ranking público destacando empresas e organizações com as melhores práticas de governança em proteção de dados

Justificativa: A prática de rankings é muito questionável por acabar favorecendo empresas que influenciam o executor do ranking. Salvo se esse ranking for feito pelo governo (ANPD) com transparência para a população.

Subsídios adicionais:

1. Empresas e administração pública, fornecer dados às representações de trabalhadores, a fim de auxiliar em negociações, processos jurídicos, processos administrativos, transparência em conflitos e melhoria das condições de trabalho, para qualquer tipo de atividade laboral e qualquer tipo de contrato, considerando trabalhadores no regime da CLT, prestadores de serviços autônomos, trabalhadores plataformizados ou qualquer outra forma de trabalho subordinado.

2. Os produtos de IA, como escores e reconhecimento biométrico, mesmo quando tecnicamente capazes de evitar a identificação direta de uma pessoa natural, não impedem que o sistema produza resultados que afetem o titular dos dados utilizados. A anonimização, embora atue nos símbolos dos dados pessoais que possam identificar um indivíduo, não altera os padrões dos dados em relação a outros ou a si mesmos ao longo do tempo. Portanto, independentemente da adequação dos processos de anonimização, é crucial analisar constantemente os efeitos dos produtos de dados, não apenas para prevenir violações aos direitos do cidadão, mas também para promover ativamente todos os direitos
3. Constante monitoramento ativo do setor privado e público, em relação aos efeitos da aplicação dos dados pessoais em seus produtos e serviços, a garantia de direitos relacionados a privacidade, proteção de dados e qualquer outro direito adquirido pelos titulares de dados.
4. Incentivar o desenvolvimento de modelos de IA explicáveis permite que decisões automatizadas possam ser compreendidas e contestadas pelos titulares de dados quando necessário e trazendo segurança jurídica para os produtores;