FGV DCI
DIRETORIA DE CONTROLES INTERNOS

GUIA DE PROTEÇÃO DE DADOS PESSOAIS

CHATBOTS

CC.04.002.2024

OUTUBRO, 2024

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CHATBOTS

VERSÃO 1.0 – OUTUBRO, 2024.

FICHA TÉCNICA

Diretoria de Controles Internos – DCI
Maria Alice da Justa Lemos
Diretora de Controles Internos

Analista responsável por este Guia:
Alessandra Rigueti Barcellos

Jordan Vinícius de Oliveira
Encarregado de Proteção de Dados Pessoais

Equipe Extracontratual:

Laila Sá Ferreira
Taís Povill Rocha
Alessandra Rigueti Barcellos
Nadja Nayra da Cruz Ferreira Ribeiro

AVISO LEGAL

Este Guia foi elaborado pela Equipe do Encarregado de Proteção de Dados Pessoais da Fundação Getulio Vargas – FGV e tem como objetivo o compartilhamento de conhecimento envolvendo a conformidade de atividades de tratamento de dados pessoais para o tema escolhido.

O presente documento possui intuito meramente informativo, não sendo utilizado para fins de exploração comercial e apresenta a devida referência na página 2. Do mesmo modo, este documento não deve ser considerado como aconselhamento jurídico e não substitui a avaliação de uma equipe profissional de proteção de dados para cada caso.

SUMÁRIO

1. CONTEXTUALIZAÇÃO

O presente Guia é um dos frutos do projeto de adequação da Fundação Getulio Vargas – FGV em relação à Lei Geral de Proteção de Dados ("LGPD"), aprovada em agosto de 2018, e outras leis setoriais sobre o tema.

A LGPD é aplicável a qualquer operação de tratamento de dados pessoais, seja ela realizada por pessoa natural, pessoa jurídica de direito privado ou pessoa jurídica de direito público. Na condição de Instituição de Ensino Superior ("IES"), a FGV desenvolve, entre outras atividades, operações de caráter administrativo, acadêmico e educacional (como por exemplo, a necessidade de guarda permanente de históricos escolares, provas, realização de pesquisas, desenvolvimento de projetos etc.). Nesse sentido, na condição de Instituição Educacional, a FGV deverá observar as obrigações normativas específicas das entidades públicas reguladoras, como, por exemplo, o Ministério da Educação ("MEC") e a Autoridade Nacional de Proteção de Dados (“ANPD”).

Assim, a FGV desenvolveu, em maio de 2019, um projeto para cumprir com os objetivos de sua conformidade regulatória perante as leis de proteção de dados, denominado **Projeto Presidência - Implantação do Programa de Conformidade: Leis de Proteção de Dados Pessoais (“Projeto”)**. Esta iniciativa, entre outras atividades, buscou parametrizar ações de conformidade da FGV ao novo contexto regulatório de proteção de dados, bem como, a partir das lições aprendidas, fornecer subsídios e materiais de apoio ao setor educacional.

Após a conclusão do Projeto inicial, a FGV criou a **Equipe do Encarregado de Proteção de Dados Pessoais**, no âmbito de sua Diretoria de Controles Internos ("DCI"). Esta Equipe tem como finalidade principal manter a FGV em adequação às normas de proteção de dados aplicáveis às suas atividades, bem como funcionar na condição de interlocutora junto aos variados setores da Organização, à ANPD, aos titulares de dados pessoais[1] e aos demais agentes de tratamento.

O objetivo deste Guia é fornecer subsídios e diretrizes que orientem a utilização de chatbots por instituições em geral, em especial quanto à temática privacidade e proteção de dados pessoais.

[1] O titular de dados pessoais é a pessoa natural à qual o dado pessoal se refere.

2. AFINAL: O QUE É UM CHATBOT?

Em uma era cada vez mais tecnológica e digital, o desenvolvimento de soluções inovadoras ocorre de forma acelerada. O que pode ter sido inovador ontem, amanhã provavelmente estará ultrapassado.

A corrida acelerada por inovação tecnológica tem sido uma verdadeira arena entre muitas empresas em busca de reconhecimento internacional. Um exemplo, no ano de 2023, foi o acirramento da disputa entre Microsoft e Alphabet (Google) pela vanguarda no desenvolvimento de agentes de conversação baseados em inteligência artificial[2]. Mas, afinal, o que são esses tais agentes de conversação comumente chamados "chatbots"?

De modo simples, um chatbot é "um programa de computador que simula e processa conversas humanas (escritas ou faladas), permitindo que as pessoas interajam com dispositivos digitais como se estivessem se comunicando com uma pessoa real"[3]. Ou seja, é um mecanismo automatizado de conversa, em que é possível a um usuário fazer perguntas e obter respostas geradas automaticamente, sejam elas supervisionadas por humanos, ou não.

Dentre muitas funcionalidades possíveis, os chatbots são capazes de esclarecer dúvidas; permitem às empresas a construção e o fortalecimento de relacionamentos entre os colaboradores e com os clientes; e podem ser, também, instrumentos eficazes para a tomada de decisão dos gestores.

Diante de tantos benefícios e a demanda crescente nas instituições por inovação tecnológica, é preciso ligar o alerta e ter muita cautela quanto à escolha do melhor modelo de chatbot a ser utilizado de acordo com o objetivo a ser alcançado por uma instituição.

Muitas instituições, no afã de não ficarem para trás na corrida tecnológica, faltam com a devida análise de risco que as ferramentas exigem. Este guia se propõe justamente a elucidar questões cruciais quando levada em consideração a temática privacidade e proteção de dados pessoais, em especial no que se refere às disposições legais contidas na LGPD e orientações vigentes da ANPD. Para isso, entender as funcionalidades e riscos de cada tipo de chatbot é fundamental.

[2] Nicole Goodkind. *Google e Microsoft brigam pelo futuro da inteligência artificial*. CNN Brasil, 2023. Disponível em <link>. Acesso em: 21 dez. 2023.
[3] O que é um chatbot? Oracle. Disponível em <link> Acessado em 28 jun. 2024.

2.1. CONCEITOS PRELIMINARES

Antes de aprofundar o estudo sobre classificações, aplicações e riscos na utilização de chatbots, a fim de auxiliar a compreensão, é preciso, inicialmente, passar brevemente por conceitos como **(i) algoritmo, (ii) processamento de linguagem natural (PLN) e (iii) aprendizado de máquina (machine learning – "ML")**. Reconhecendo a sua amplitude e o aprofundado estudo que cada conceito exige, esclarece-se que este Guia se propõe a elucidá-los de forma objetiva e com a finalidade principal de assessorar o estudo do tema privacidade e proteção de dados em chatbots.

Algoritmos: instruções básicas

Inicialmente, é importante analisar a definição de algoritmo:

DEFINIÇÃO

ALGORITMO

1. "Uma sequência de instruções que diz a um computador o que fazer"[4].
2. "Um procedimento ou conjunto de instruções e regras para performar uma tarefa específica ou resolver um problema particular resolvendo um computador[5].

No caso de chatbots, em geral, o conjunto dessas instruções ou regras é desenhado especificamente para viabilizar a interação entre o usuário e a tecnologia. Tal tecnologia pode abranger tanto interações específicas direcionadas a um tópico/assunto (ex.: instruções ao consumidor sobre como abrir chamados em um portal de serviços) quanto interações mais abrangente (ex.: conversa sobre tópicos variados que evolui a partir de considerações prévias).

A construção desse algoritmo passa, contudo, pela capacidade do chatbot em compreender o modo humano de se comunicar, especialmente consideradas as peculiaridades da linguagem escrita ou da linguagem oral, onde o conceito de processamento de linguagem natural se torna útil.

[4] Domingos, Pedro. *A Revolução do Algoritmo Mestre – Como a Aprendizagem Automática está a mudar o mundo.* 5ª Edição, Lisboa. Editora Manuscrito, 2018.
[5] IAPP. *Key Terms for AI Governance*. International Association of Privacy Professionals. Disponível em <link>. Acessado em 27 set. 2024.

Processamento de linguagem natural: compreensão da linguagem

A comunicação humana é dotada de diversas peculiaridades: o idioma, o tom de escrita ou fala, o significado e a ordem das palavras ou mesmo o modo de se expressar, seja na forma escrita ou oral: todas essas nuances interferem no sucesso da comunicação entre homem e computador.

Desse modo, o processamento de linguagem natural (PLN) emprega recursos como os de semântica (significado das palavras em determinado contexto), sintática (organização de sentenças dentro das regras de gramática), reconhecimento de fala, entre outros, para organizar e estruturar a interação com um humano.

O PLN pode ser entendido como uma ramificação da ciência computacional que, atualmente, representa um dos maiores desafios no desenvolvimento de chatbots. Isso se deve à complexidade da comunicação humana. Palavras sinônimas, conteúdos com ironia, contextos culturais e análise de sentimento podem ser de difícil decodificação pela máquina. O entendimento e processamento errados dos dados podem gerar uma série de consequências graves, principalmente no que tange à discriminação de grupos vulneráveis, "alucinações" e informações falsas/erradas pelo chatbot. Estes riscos serão abordados no tópico *3.3 Tratamento de Dados Pessoais em Chatbots*.

Uma vez compreendido que o desenho de chatbots passa por conjuntos de regras de interação (algoritmos) que levam em conta a compreensão da linguagem humana (processamento de linguagem natural), um elemento essencial para a sua compreensão é o do nível de aprendizado empregado.

Aprendizado de máquina: aperfeiçoamento retroalimentado

De forma simples, a noção de aprendizado de máquina decorre de três componentes: T (tarefa), E (experiência) e P (performance), sendo que um sistema ou solução "aprende" na medida em que a experiência o torna mais preciso em uma dada tarefa, de modo que a sua performance melhore ao longo do tempo[6].

Imagine, por exemplo, um chatbot cuja *tarefa* seja auxiliar um usuário quanto à redação de cláusulas em contratos de propriedade intelectual. Na primeira interação, o comando inserido pelo usuário ao modelo solicitou que ele "listasse cláusulas gerais de CC aplicáveis a contratos de direito autoral", havendo imprecisão na resposta fornecida devido à falta de definição sobre o que seria "CC" (como

[6] MITCHEL, Tom M. *Machine Learning*. Nova Iorque: McGraw-Hill, 1977. 414p.

Código Civil ou *Creative Commons*). Após a especificação do usuário de que seu desejo era o de cláusulas de licenças *Creative Commons*, o modelo "aprendeu" essa nova definição e utilizará essa informação adquirida na *experiência* com o usuário para fornecer respostas cada vez mais precisas, o que melhorará sua *performance.*

Assim, um ponto crucial para a compreensão de chatbots é a de que nem todo o conjunto de regras da tecnologia utilizada empregará aprendizado de máquina (como, por exemplo, os chamados *large language models*, algoritmos sofisticados alimentados com grandes volumes de dados capazes de entender e criar conteúdo seguindo determinados padrões).

Alguns modelos, mais simples, basicamente restringem o funcionamento de seu algoritmo a algumas sequências de instruções limitadas e não podem oferecer experiências mais personalizadas ou acessar bancos de dados contendo dados pessoais para oferecer respostas personalizadas. Outros, contudo, não apenas poderão oferecer experiências personalizadas como sugerir novos conteúdos não previsíveis pelos criadores.

Logo, sob o ponto de vista de riscos em chatbots, é imprescindível compreender o tipo de tecnologia em uso para identificar o grau de risco e quais as ações de conformidade serão necessárias a partir de leis de proteção de dados pessoais, como a LGPD.

2.2. CLASSIFICANDO CHATBOTS

Conforme já abordado, a utilização de chatbots para as mais variadas funções no contexto de instituições tem se tornado uma realidade cada vez mais comum e essencial. Relacionamento com o cliente, automação de tarefas, recuperação de informações, integração de sistemas de pagamento e assistentes virtuais são exemplos de como é possível otimizar o trabalho humano com o auxílio desses agentes automatizados. Contudo, cada funcionalidade exige uma atenção específica, em especial, quando o assunto é tratamento de dados pessoais.

Desse modo, antes de desenvolver um chatbot para atender a uma determinada função em uma instituição, é preciso previamente entender qual é a finalidade específica que se espera da ferramenta e o que é essencial para a realização da atividade. A partir dessa análise bem estabelecida, é possível escolher o melhor modelo de chatbot a ser desenvolvido sem que, para isso, a atividade seja exposta a um grau de risco desnecessário.

PONTO DE ATENÇÃO

Muitas instituições, tomadas pela euforia de utilizar ferramentas com inteligência artificial esquecem de realizar previamente uma análise de risco e retorno. As perguntas abaixo são alguns exemplos do que deve ser questionado antes de desenvolver/contratar um serviço de chatbot:

1) Para que eu preciso dessa ferramenta?

2) O que é efetivamente necessário nessa atividade?

4) Quais os agentes (internos e externos) terão acesso a essa ferramenta?

5) Haverá a conexão a uma base de dados pessoais que poderá fornecer informações de volta ao usuário?

6) É possível que a ferramenta seja alvo de utilizações não previstas? Em caso positivo, como prevenir e remediar essa situação?

Como falado, existem diferentes tipos de chatbots aptos a atender finalidades variadas. Ao entendermos cada tipo de abordagem e classificação é possível ter clareza sobre qual tipo é de fato o mais interessante e vantajoso de acordo com a finalidade almejada pela instituição e, ainda, o que pode representar maiores riscos a privacidade de seus usuários.

Um estudo desenvolvido por O. Trofymenko, Y.V. Prokop, A. Zadereyko e N. Loginova em 2021[7] estabelece alguns dos critérios mais utilizados para classificar chatbots. Para fins de estudo deste Guia, abordaremos, de forma resumida, as seguintes classificações: (i) por finalidade; (ii) por localização; (iii) por tipo de interface; e (iv) por algoritmo. É importante frisar, desde já, que um tipo de classificação não exclui a outra, de modo que as classificações são apenas diferentes abordagens para entender as funcionalidades dos chatbots. Abaixo segue a descrição de cada classificação.

(i) Por finalidade

Este conceito subdivide os chatbots em dois tipos: aqueles cujo propósito é desenvolver uma conversa com ampla variedade de tópicos, sem um objetivo claro e; os que são focados em um tópico específico e bem delimitado, voltado à resolução de uma determinada demanda, sem variedade de assunto.

[7] O. Trofymenko, Y.V. Prokop, A. Zadereyko e N. Loginova. *Classification of Chatbots*. Odesa, Ucrânia. 2021. Disponível em <link>. Acessado em 04 jan. 2024.

Adianta-se que, quanto mais liberdade para o desenvolvimento de uma conversa, maiores deverão ser as medidas de segurança e mitigação de riscos. Quando o chatbot não possuir um propósito delimitado, ainda assim é importante estabelecer limites para a interação com o usuário, a fim de impedir que ele dê respostas erradas/falsas ou, ainda, replique um diálogo com expressões que fujam à urbanidade e atentem contra a dignidade humana. Um chatbot desenvolvido para lidar com alunos em uma Instituição Educacional, por exemplo, deve se ater aos temas específicos relacionados à demanda que se propõe a solucionar.

(ii) Por localização

Nesta classificação, os chatbots podem estar inseridos em páginas da web (site da instituição, por exemplo), em interfaces de mensageria (WhatsApp, Telegram, Signal, etc) ou aplicativos/softwares específicos como, por exemplo, de prestação de serviço de entrega de comida, entrega de encomenda, etc. Aqui, um dos principais pontos de atenção está relacionado ao desenvolvimento de um chatbot em plataformas de empresas terceiras, que dispõem de regras próprias muitas vezes relacionadas ao seu país de origem e ainda, às suas políticas e termos de uso.

Assim, a título exemplificativo, quando uma instituição optar por inserir um chatbot no aplicativo WhatsApp do Grupo Meta, além de observar a LGPD e demais legislações aplicáveis, a depender do contexto a ser utilizado, é fundamental que sejam observados os termos de uso, políticas e demais regras estabelecidas por este grupo, a fim de prevenir possíveis penalidades pelo mau uso ou uso inadequado da ferramenta, o que pode acarretar verdadeiro prejuízo para a instituição.

(iii) Por tipo de interface

Um outro tipo de classificação que foi pontuada no estudo de O. Trofymenko, Y.V. Prokop, A. Zadereyko e N. Loginova, foi a classificação por interface. Esta classificação pode ser subdividida em “botão”, onde o usuário apenas seleciona uma opção dentre uma lista pré-definida na conversa; “texto”, onde é possível que o usuário escreva na conversa e então seja respondido (o que demanda maior complexidade na programação do chatbot); “modelo misto” onde os dois tipos de interface podem ocorrer; e por voz, onde é possível dialogar com o chatbot, como por exemplo, atendimento por “robô eletrônico”. Este último tipo de interface envolve certo nível de desenvolvimento do chatbot, uma vez que a mensagem passada por comando de voz será decodificada para texto, analisada e, por fim, respondida.

Em termos de tratamento de dados pessoais, conforme se verá mais adiante, é aconselhável – sempre que possível e a depender da finalidade – utilizar interfaces com botões e sem a necessidade de elaboração de texto livre pelo usuário, que pode fornecer informações pessoais desnecessárias à finalidade da ferramenta.

Pontua-se, ainda, que quanto mais desenvolvido o nível de interação com o usuário, maiores serão os custos envolvidos e maiores devem ser as medidas de mitigação de riscos, uma vez que ferramentas que processam grande número de dados são maiores alvos para hackers mal-intencionados.

Um exemplo de uma boa medida de mitigação para ser adotado em qualquer chatbot que trate dados pessoais, em especial para interfaces que possuam conexão com bases de dados de clientes ou pessoas em geral, é a implementação de fatores de autenticação e certificação de identidade do usuário, como duplo fator de autenticação com envio de senha para o número de celular da pessoa para prosseguir a conversa.

(iv) Por algoritmo

Esta classificação se subdivide em chatbots simples, inteligentes e híbridos. Os chatbots simples possuem uma interação pré-configurada, com possíveis respostas previamente determinadas em um script em que o usuário precisará utilizar as palavras-chave registradas na programação do chatbot para uma resposta satisfatória. Já os chatbots inteligentes possuem a conversação aprofundada pelo treinamento com grandes bases de dados, utilizando, ainda, aprendizado de máquina para desenvolver sua conversação. Os chatbots híbridos são uma combinação dos dois tipos de chatbots anteriores, onde há uma árvore de respostas bem estruturada e, ainda, é possível a utilização de IA para extração de dados informados na conversa.

Neste tipo de classificação, sem dúvidas, a principal preocupação se relaciona aos chatbots inteligentes ou híbridos. Isso porque, precisam ser treinados com grandes bases de dados e, em termos de dados pessoais e autorais, devem observar as permissões necessárias conforme determina a legislação. Ainda, é preciso garantir a legitimidade do acesso a esses dados de treinamento, como a observância de uma base legal válida e o conhecimento dos titulares a respeito de seu uso.

Outra preocupação a ser pontuada em chatbots inteligentes/híbridos é a possibilidade de apresentar vieses. A depender da base de dados utilizada, o contexto cultural e histórico desses dados e correlações semânticas das palavras utilizadas para treinamento do chatbot é possível que haja enviesamento. Nesses casos, além da preocupação com o comportamento da tecnologia, é imprescindível avaliar qual o grau de representatividade das bases de dados utilizadas para treinar os modelos, evitando-se sempre a discriminação ilícita de pessoas ou grupos.

Existem variados tipos de categorização de chatbots e não é a pretensão deste Guia esgotá-los em suas peculiaridades. Contudo, é importante deixar claro que certos tipos podem gerar maiores preocupações quando observada a temática proteção de dados pessoais.

PONTO DE ATENÇÃO

Quanto menor o tratamento de dados pessoais, ou ainda, quando não há o tratamento de dados pessoais, não ensejará maiores preocupações por parte das instituições. Porém, algumas funcionalidades devem ligar o **alerta**: **excesso de tratamento de dados pessoais, tratamento de dados pessoais sensíveis, necessidade de compartilhamento de dados com outras instituições (podendo ser estrangeiras) sem salvaguardas de proteção de dados, decisões automatizadas não supervisionadas e chatbots de livre diálogo com o usuário** são alguns exemplos que demandam cuidados por parte das instituições.

Após entendidos os conceitos iniciais relacionados a chatbots, sua definição e classificações, é fundamental entender quais os riscos relacionados à proteção de dados pessoais e como preveni-los e mitigá-los de acordo com a LGPD, conforme aprofundado no capítulo a seguir.

RESUMO

NESTE CAPÍTULO, ENTENDEMOS QUE:

- Um chatbot é um programa de computador que simula e processa conversas humanas (escritas ou faladas), permitindo que as pessoas interajam com dispositivos digitais como se estivessem se comunicando com uma pessoa real.
- Ainda no item 2.1 foram propostos alguns conceitos preliminares ao estudo de chatbots, como algoritmo, processamento de linguagem natural e aprendizado de máquina.
- Por fim, no item 2.2, foram propostas algumas classificações de modelos de chatbots, como por tipos de finalidade, localização, interface e algoritmo. Aqui foi

listada a importância de se identificar pontos de risco, como a conexão do chatbot com uma base de dados pessoais ou o nível de liberdade do usuário na interação (ex.: texto livre).

3. PROTEÇÃO DE DADOS PESSOAIS EM CHATBOTS

Neste capítulo, ao abordar o tratamento de dados pessoais em chatbots é importante que seja compreendido o que pode ser definido como dado pessoal, o que caracteriza o seu tratamento e quais princípios devem ser observados.

Cumpre esclarecer, desde já, que nem todo chatbot tratará dados pessoais. Por este motivo é tão importante que seja feita uma minuciosa análise da finalidade e funcionalidade de um chatbot a ser desenvolvido/contratado no âmbito de uma instituição, pois, a depender da atividade, não havendo a necessidade de tratamento de dados pessoais, a LGPD sequer será aplicável.

Neste capítulo também serão abordados os níveis de responsabilização de uma instituição quando o assunto é tratamento de dados pessoais[8], o que é de suma importância, pois em muitos casos os chatbots são desenvolvidos e aplicados por mais de uma instituição, havendo o tratamento de dados pessoais sob escopos de atuação diferentes.

A partir dessas definições bem estabelecidas será possível aprofundar o estudo do tratamento de dados pessoais em chatbots, riscos e pontos de cautela específicos conforme determina a LGPD.

[8] Sobre a responsabilização dos agentes de tratamento de dados pessoais é imperioso observar a atuação das Autoridades de Proteção de Dados em diversos países, que podem aplicar sanções severas em caso de desconformidade com seu regulamento de proteção de dados. A título exemplificativo, em março de 2023 a autoridade de proteção de dados italiana (Garante) determinou o bloqueio do ChatGPT no país por período de 20 dias, sob a acusação de coleta ilegal de dados de usuários e permissão de acesso indevido para menores de idade. Além do prejuízo financeiro estimado, a empresa responsável OpenIA precisou implementar em 20 dias uma série de mudanças a fim de adaptar a ferramenta ao regulamento europeu. Notícia disponível em <link>. Acessado em 30 jan. 2024.

3.1. DEFINIÇÕES E PRINCÍPIOS DE PROTEÇÃO DE DADOS PESSOAIS

De acordo com a LGPD, dado pessoal é aquele capaz de tornar uma pessoa identificada ou identificável. Apesar de aparentemente simples, é preciso cautela quando abordamos dados gerados, por exemplo, no ambiente online. Dados de geolocalização, dados dos dispositivos de seus usuários, e "identificadores online" também podem ser considerados dados pessoais, na medida em que são capazes de identificá-los, ainda que não revelem diretamente o seu nome.

No contexto brasileiro, vale pontuar o disposto no Decreto 8.771/2016, em seu artigo 14, inciso I, que definiu dado pessoal (antes da entrada em vigor da LGPD) como "dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa" (grifado).

Mas a definição de dado pessoal não para por aí. A LGPD, em seu art. 5º, inciso II dispôs de forma taxativa alguns dados pessoais que merecem especial atenção, chamados de dados pessoais sensíveis por possuírem maior grau de resistividade em seu uso. Assim, dados de origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural são definidos como dados pessoais sensíveis.

Desse modo, registra-se o primeiro ponto de alerta: caso o chatbot a ser desenvolvido precise realizar o tratamento de dados pessoais sensíveis, observada a sua finalidade, algumas medidas de segurança a mais deverão ser levadas em consideração. Mas, não é só isso... uma fase preliminar a qualquer tratamento de dado pessoal, seja ele sensível ou não, é a escolha da base legal aplicável.

De acordo com a LGPD, toda a atividade que envolva o tratamento de dados pessoais deverá ter uma base legal válida. Ou seja, a atividade precisará ter uma fundamentação legal que a justifique. As bases legais são hipóteses autorizativas para o tratamento de dados pessoais. Na LGPD elas estão descritas no artigo 7º e 11.

Voltando ao exemplo do tratamento de dado sensível, as hipóteses autorizativas estão previstas especificamente no art. 11 da referida lei. Assim, o tratamento de dados pessoais sensíveis somente poderá ser realizado em chatbots quando houver a previsão legal estabelecida neste artigo.

Mas afinal, o que podemos considerar como tratamento de dados pessoais?

DEFINIÇÃO

TRATAMENTO DE DADOS PESSOAIS

De acordo com o art. 5º, X da LGPD, tratamento de dados pessoais é toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Desse modo, a simples inserção de nome do usuário ao interagir com um chatbot já configuraria o tratamento de dados pessoais pela LGPD. Ainda, o simples acesso visual ao dado informado, o armazenamento do dado em um sistema interno, ou o compartilhamento com terceiros, são considerados tratamento de dados pessoais.

Uma vez entendido o que é dado pessoal, dado pessoal sensível, base legal e tratamento de dados pessoais, passemos a abordar os princípios da LGPD, norteadores fundamentais de todo tratamento de dados pessoais.

Assim como em outros diplomas legais, a LGPD também estabelece princípios basilares que devem guiar todo e qualquer tratamento de dados pessoais. De acordo com o art. 6º do referido diploma legal, além da boa-fé, deverão ser observados os princípios da (i) finalidade; (ii) adequação; (iii) necessidade; (iv) livre acesso; (v) qualidade dos dados; (vi) transparência; (vii) segurança; (viii)prevenção; (ix) não discriminação e; (x) responsabilização e prestação de contas. Adiante, segue um quadro explicativo com os princípios elencados na LGPD:

Princípio	Descrição do art. 6º da LGPD
Finalidade	Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades
Adequação	Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento
Necessidade	Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados

Livre acesso	Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais
Qualidade dos dados	Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento
Transparência	Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial
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
Prevenção	Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais
Não discriminação	Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos
Responsabilização e prestação de contas	Demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas

Ao desenvolver ou contratar uma ferramenta de chatbot é imprescindível fazer um checklist destes princípios, cuja não observância representa verdadeiro risco para o titular de dados e, ainda, risco interno para a instituição como, por exemplo, a incorrência em sanções pela ANPD, a diminuição de competitividade no mercado por baixo nível de compliance, eventual reprovação pelo usuário final da ferramenta ao constatar a ausência de conformidade, dentre outras consequências que representam elevado prejuízo às instituições.

Agora, passaremos a uma breve explicação sobre agentes de tratamento de dados pessoais e suas responsabilidades.

3.2. AGENTES DE TRATAMENTO E SUAS RESPONSABILIDADES

De acordo com a LGPD, as responsabilidades pelo tratamento de dados pessoais são delimitadas entre dois perfis de agentes de tratamento: (i) o controlador de dados pessoais e (ii) o operador de dados pessoais.

Em definição objetiva disposta no art. 5º, VI da LGPD, o controlador é a "*pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais*". Já o operador é a "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador".

Ou seja, o operador de dados deverá sempre observar as orientações de tratamento de dados definidas pelo controlador. Este, por sua vez, delimitará as bases legais e finalidades de tratamento de dados pessoais, bem como outras responsabilidades dispostas na LGPD, como, por exemplo, a elaboração de relatório de impacto à proteção de dados pessoais (art.10, §3º e art. 38 da LGPD) e a comunicação de incidentes com dados pessoais à ANPD e aos titulares (art. 48 da LGPD).

Ter esses conceitos bem definidos é importante quando há a intenção de contratar um serviço ou desenvolver internamente um chatbot, seja de atendimento ao cliente, seja de gerenciamento de tarefas, ou qualquer outra funcionalidade aplicável.

Qualquer agente externo à instituição que tenha acesso aos dados pessoais tratados no âmbito das funcionalidades do chatbot precisa estar adequado à legislação e às normas de privacidade da empresa. Ainda, é preciso informar ao titular de dados que há o tratamento de dados pessoais realizado por um terceiro agente de tratamento. Este, a depender do tipo de tratamento, deverá ser identificado como controlador ou operador de dados pessoais.

Um operador de dados pessoais, que fornece o serviço do chatbot em um aplicativo de mensageria, por exemplo, deve se restringir ao tratamento estabelecido em contrato, observando principalmente as finalidades propostas pelo controlador de dados pessoais. Qualquer finalidade diversa do tratamento de dados pessoais poderá ser considerada incompatível com a LGPD e passível de sanção pela ANPD.

Para aprofundamento do tema de agentes de tratamento recomenda-se a leitura do **Guia de Agentes de Tratamento de Dados Pessoais** disponível no Portal de Proteção de Dados da FGV (link aqui).

3.3. TRATAMENTO DE DADOS PESSOAIS EM CHATBOTS

Conforme já abordado, nem todo chatbot tratará dados pessoais. Uma vez que ocorra, é preciso observar todas as medidas legais e de segurança necessárias. Caso o chatbot da sua instituição trate dados pessoais, é importante mapear todo o processo de tratamento: perguntas como quais dados pessoais serão tratados, qual a projeção de pessoas alcançadas, se haverá compartilhamento de dados e quantas pessoas terão acesso são primordiais para a análise de risco.

Para aprofundar o estudo sobre o processo de mapeamento de tratamento de dados pessoais sugere-se a leitura do **Guia de Relatório de Impacto de Proteção de Dados** disponível no Portal de Proteção de Dados da FGV (link aqui).

Em recente publicação da autoridade francesa de proteção de dados (Commission Nationale de l'Informatique et des Libertés – CNIL) foram disponibilizadas dicas e recomendações sobre o desenvolvimento de sistemas de inteligência artificial a fim de auxiliar as instituições a observarem a regulamentação de proteção de dados pessoais europeia (GDPR)[9]. Apesar de focado no contexto europeu e em sistemas de IA, o passo a passo pode auxiliar na implementação de um chatbot.

Segundo o documento, os passos a serem observados são: 1) determinação do regime jurídico aplicável; 2) definição de um propósito/finalidade; 3) estabelecer a qualificação legal dos provedores de sistemas de IA (se controladores ou operadores); 4) garantir a licitude do tratamento dos dados; 5) realização de uma avaliação de impacto sobre a proteção de dados, quando necessário e; 6) levar em conta a proteção de dados nas escolhas de design do sistema.

Um ponto importante a ser destacado quando se aborda o tratamento de dados pessoais em chatbots é que, a depender do tipo de chatbot utilizado, conforme exemplificado no capítulo 2, será necessário traçar medidas de segurança adequadas ao tratamento de dados pessoais realizado.

Frisa-se que existe uma variedade de medidas de segurança possíveis de serem implementadas conforme a complexidade do tratamento. Assim, recomenda-se que a contratação e/ou o desenvolvimento do chatbot seja objeto de acompanhamento de profissionais de segurança da informação e de privacidade desde o início do projeto. A seguir, serão abordadas algumas dicas de segurança a serem observadas ao implementar um chatbot.

[9] FRANÇA. Commission Nationale de l'Informatique et des Libertés (CNIL). *Fiches pratiques sur l'IA*, 2024. Disponível em: <link>. Acessado em 12 abr. 2024.

3.3.1 MEDIDAS DE SEGURANÇA

A título exemplificativo, é possível pontuar de forma simplificada algumas medidas de segurança comumente utilizadas, que podem servir como sugestão caso sua instituição pretenda implementar um chatbot. Entretanto, reitera-se a necessidade do acompanhamento de especialistas com expertise em segurança da informação e privacidade de dados.

i) Implementação de autenticação de identidade do usuário

Um ponto crucial para garantir a segurança dos dados é a autenticação da identidade do usuário, em especial quando há a previsão do sistema se conectar a uma base de dados pessoais ou dados sigilosos para fornecer informações de volta ao usuário. Essa autenticação deve ser feita por métodos seguros, como exigência de login ou verificação de OTP (*One Time Password*) via canal de contato informado (e-mail ou celular, por exemplo). Para chatbots cuja interação não requeira conexão a uma base de dados pessoais ou dados sigilosos, a autenticação pode ser desnecessária.

ii) Uso de criptografia especialmente em trânsito

A criptografia é basicamente uma técnica que transforma informações em um formato ilegível para pessoas sem acesso autorizado aos dados. Para isso, há um processo de codificação que torna os dados incompreensíveis, a menos que alguém possua a chave certa para decifrá-los. Há diversos graus e tipos de criptografia e sua complexidade poderá variar de acordo com o grau de risco em torno dos dados tratados. Um exemplo comumente usado em mensagens, é a criptografia de ponta a ponta (E2EE) para trânsito das informações (ou seja, do terminal/dispositivo de origem ao de destino, garantindo que terceiros que interceptem a mensagem não consigam tornar seu conteúdo legível), onde apenas as partes comunicantes podem ler as mensagens[10].

iii) Restrição de Acesso

Internamente, a restrição de acesso aos dados tratados pelo chatbot também se caracteriza como uma medida de segurança eficaz e pode ocorrer de diversas formas. Aqui, o princípio do menor privilégio deve ser sempre observado, ou seja, a busca para garantir que apenas o mínimo de pessoas/colaboradores tenha acesso aos dados da interação do chatbot. O raciocínio é simples: quanto menor o número de pessoas que precise ter apenas acesso aos dados, menor o risco de ocorrência de algum incidente de segurança com eles.

[10] H. Martin, N. Jana, A. Saghair Khalifa, A. Hussam, S. Václav, O. Lidia. *Chatbots: Security, privacy, data protection, and social aspects*. Ostrava, República Checa. 2021. Disponível em <link>. Acessado em 25 abr. 2024.

iv) Termo de Sigilo e Confidencialidade

Outra medida de segurança importante é a implementação de um termo de confidencialidade para assinatura dos colaboradores que acessem os dados tratados no âmbito do chatbot. Assim, será efetivado um compromisso maior dos responsáveis sobre o tratamento daqueles dados.

v) Aviso de Privacidade e Termos de Uso

A disponibilização de um aviso de privacidade e termos de uso é uma medida importante para evidenciar a transparência. Esses documentos devem informar como ocorre a interação do chatbot com o usuário, quais dados são tratados, qual finalidade, a existência de compartilhamento e as medidas de segurança adotadas, por exemplo. Além de evidenciar a conformidade da ferramenta, orientam o usuário em caso de dúvidas e, ainda, como ele deve agir em caso de algum incidente.

vi) Cuidados com armazenamento das interações e transferência internacional de dados

Por vezes, os chatbots se utilizam de infraestrutura de tecnologia da informação mantida fora do país, inclusive com armazenamento das conversas em servidores internacionais regulados por outras legislações que não apenas a LGPD. Nessas situações, é importante tomar cuidado com o nível de proteção das informações (inclusive sobre a sensibilidade das conversas e se há necessidade de uso de criptografia em repouso) e com o local/jurisdição onde ficarão armazenadas para evitar surpresas desagradáveis com o uso do histórico de conversas por terceiros.

Por fim, frisa-se que as medidas de segurança indicadas, são meros exemplos, não exaustivos e pontuados de forma simplificada, de ações que podem ser tomadas para garantir um mínimo grau de segurança quando se pretende implementar um chatbot.

3.3.2 COMPARTILHAMENTO DE DADOS PESSOAIS EM CHATBOTS

Um ponto importante a ser abordado ao falar sobre tratamento de dados pessoais em chatbots é o compartilhamento de dados com empresas parceiras e/ou fornecedores e prestadores de serviço. Não é raro, por exemplo, que os dados coletados em conversa sejam armazenados em um ambiente de nuvem[11] terceirizado. Como garantir, nesses casos, que a empresa contratada para armazenar os dados está em conformidade com a LGPD?

[11] Armazenamento de arquivos na Internet por meio de infraestruturas, plataformas ou software hospedados por outros fornecedores.

Apesar de ser o cenário ideal, às vezes não é simples estabelecer cláusulas contratuais específicas com obrigações relacionadas ao tratamento de dados pessoais. Muitas vezes pode haver uma difícil negociação dos termos contratuais. Ainda que isso ocorra, é imprescindível observar atentamente as disposições contratuais sobre o tratamento de dados pessoais e garantir o cumprimento dos regulamentos de proteção de dados pessoais.

Observar se a empresa possui políticas que assegurem a proteção de dados pessoais, medidas de segurança compatíveis às atividades e setor específico que garanta o compliance com as normas vigentes, são exemplos de ações que demonstram a conformidade da instituição contratada.

Ainda, é importante cientificar o cliente cujos dados estão sendo compartilhados, informar a finalidade deste compartilhamento e, sempre que possível, a instituição que receberá estes dados. Quando este compartilhamento ocorre para instituições estrangeiras, alguns cuidados especiais deverão ser tomados, conforme abordado a seguir.

3.3.3 TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS

Ao falar em compartilhamento de dados no âmbito da operação de chatbots é imprescindível passar pelo conceito de transferência internacional de dados, pois a depender do suporte operacional e software da ferramenta, provavelmente países estrangeiros estarão envolvidos no fluxo de dados.

Nos termos do art. 5°, XV da LGPD, entende-se como transferência internacional o fluxo de "(...) dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro". Ainda, citando o tema no âmbito da União Europeia, o GDPR - Regulamento Geral de Proteção de Dados Europeu define este processo como "Qualquer transferência de dados pessoais tratados após a transferência para um país terceiro ou para uma organização internacional (…)"[12].

É importante diferenciar o mero transporte das informações pessoais por meio da rede de internet, que, não se caracteriza por si só, como transferência internacional de dados. Assim, o provedor de internet não será considerado operador de dados apenas por viabilizar a respectiva ação.

[12] EUROPEIA, U. *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*. Jornal Oficial da União Europeia, [s.l.], n. (Atos legislativos), [s.d.]. Disponível em:<link>. Acessado em 25 abr. 2024.

Porém, diferentemente do mero transporte de dados por meio da rede de internet, quando há, por exemplo, a utilização de serviços de armazenamento em nuvem é possível que haja a transferência internacional caso o operador do serviço faça esse armazenamento fora do país, ainda que tais arquivos estejam acessíveis por meio de dispositivo com sistema operacional e acesso à Internet.

Quando houver a transferência internacional de dados pessoais na operação do chatbot é preciso se atentar para as seguintes orientações principais:

DICA

TRANSFERÊNCIA INTERNACIONAL DE DADOS NO CHATBOT

a) Observar qual dos requisitos do artigo 33 da LGPD será aplicável;
b) Disponibilizar aviso ao usuário sobre a possibilidade de transferência internacional de dados, informando para quais países ela poderá ocorrer;
c) Disponibilizar o acesso ao Aviso/Política de Privacidade das empresas estrangeiras as quais haverá a transferência internacional de dados;
d) Garantir, mediante cláusula contratual, a observância das práticas de privacidade e proteção de dados que estejam de acordo com a LGPD, orientações da ANPD e a legislação do país destinatário e que estas não sejam incompatíveis.

Para aprofundar o estudo sobre transferência internacional acesse o **Guia de Transferência Internacional de Dados**, disponível no Portal de Proteção de Dados da FGV (link aqui).

3.4. TRATAMENTO AUTOMATIZADO DE DADOS E ART. 20 DA LGPD

Conforme disposto na LGPD, o artigo 20 estabelece o direito de contestar decisões tomadas unicamente por meio do tratamento automatizado de dados pessoais, quando tais decisões impactam os interesses dos indivíduos, titulares dos dados pessoais. Esse direito se aplica, inclusive, a decisões que definem perfis pessoais, profissionais, de consumo ou de crédito, ou ainda aspectos da personalidade do indivíduo.

Curiosamente, é possível reconhecer que o direito de pleitear a revisão de uma decisão exclusivamente automatizada que impacta os direitos dos titulares de dados não foi uma novidade introduzida exclusivamente pela LGPD no sistema legal brasileiro. Conforme pontuam Renato Leite

Monteiro, Maria Cecília Gomes e Bruno Bioni, em texto produzido para a International Association of Privacy Professionals (IAPP)[13]:

> "Ele foi fornecido em relação aos modelos de credit scoring pela Lei do Cadastro Positivo juntamente com o direito à explicação, que incluiria não apenas os dados usados pelo algoritmo, mas também os critérios usados para processamento, limitados ao sigilo comercial e levando em consideração direito de propriedade intelectual. Essa estrutura foi totalmente copiada pela LGPD, mas aplicável para processamento de dados para qualquer finalidade."

A lei do Cadastro Positivo (Lei 12.414/2011) em seu artigo 5º, inciso VI, estabelece que é direito do cadastrado "solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados". Percebe-se que tanto este dispositivo legal quanto o artigo 20 da LGPD pretendem garantir o direito à transparência e, principalmente à não-discriminação. Abaixo, a fim de melhor ilustrar o direito assegurado, segue exemplo fictício de um chatbot com viés discriminatório, passível de solicitação de revisão pelo titular de dados.

EXEMPLO

AVALIAÇÃO DE PERFIL DE CRÉDITO E DISCRIMINAÇÃO

Determinada instituição financeira, a fim de agilizar o processo de concessão de crédito para clientes, desenvolveu um chatbot que faria a prévia aprovação de perfis aptos a tomar empréstimo financeiro. Um dos filtros programados no chatbot era o bairro de moradia do solicitante. Deste modo, pessoas que declaravam morar em bairros A e B eram automaticamente classificadas como potenciais devedores, por, estatisticamente, constatar-se que referidos bairros possuíam maior número de clientes maus pagadores. Desse modo, independente de o cliente comprovar fonte de renda compatível ao pagamento do empréstimo e histórico de higidez financeira, este possuía seu perfil previamente reprovado pelo chatbot.

É importante deixar claro que o direito à revisão abrange decisões **exclusivamente** baseadas em tratamento automatizado de dados. Ou seja, se a decisão for tomada com base em intervenção humana, ainda que envolva dados pessoais, o artigo 20 da LGPD não será aplicável.

[13] Bioni, Bruno; Monteiro, Renato; Oliveira, Maria Cecília. *GDPR Matchup: Brazil's General Data Protection LAW, IAPP*. 2018. Disponível em <link>. Acessado em 26 abr. 2024.

De acordo com o disposto no artigo, são passíveis de revisão as decisões automatizadas que incluem a criação de perfis pessoais, profissionais, de consumo ou de crédito com base em dados coletados; inferências sobre hábitos, preferências e comportamentos do indivíduo a partir de seus dados; e decisões que afetam diretamente a vida do indivíduo, como aprovação ou recusa de crédito, fornecimento de serviços ou produtos, etc.

Observados os aspectos elencados, uma vez que o titular de dados solicitar a revisão da decisão tomada exclusivamente de modo automatizado, de acordo com o §1º do art. 20, será responsabilidade do **controlador** de dados pessoais fornecer a explicação/revisão da decisão. Orienta-se, como uma boa prática de livre acesso, que este controlador possua um canal de comunicação adequado para esta finalidade, com acesso facilitado ao interessado.

Apesar da lei não exigir um formato específico para a solicitação, entende-se como recomendável para fins de documentação/comprovação que seja feito por escrito ou outro método passível de registro de histórico.

Cumpre esclarecer, ainda, que a LGPD não definiu um prazo específico para a solicitação da revisão disposta neste artigo. Enquanto a ANPD não se manifestar especificamente acerca do tema é importante que a instituição atue com diligência e eficiência, pois o tempo pode influenciar na efetividade da revisão e, consequentemente, no relacionamento com o interessado.

Ao abordar a análise da solicitação, muitos desafios podem surgir, ao passo que o controlador é obrigado a fornecer informações claras e adequadas sobre os critérios e procedimentos utilizados na decisão automatizada. Essa obrigação, conforme mencionado, visa garantir principalmente a aplicação do princípio da transparência e permitir que o indivíduo compreenda como a decisão foi tomada.

Ocorre que nem sempre é fácil tornar explicável o funcionamento do algoritmo responsável pela decisão... O fenômeno da “caixa preta”[14] em algoritmos complexos é um dos grandes desafios à

[14] No artigo “The black box problem revisited. Real and imaginary challenges for automated legal decision making” de Bartosz Brożek, Michał Furman, Marek Jakubiec, Bartłomiej Kucharzyk” é abordado o problema da caixa preta (“black box”) na IA e a sua explicabilidade em um contexto legal. No artigo é mencionado o problema que ocorre especialmente em IAs com machine learning (aprendizado de máquina), que são projetadas para analisar grandes padrões de dados e ao encontrar “padrões ocultos” oferecerem soluções cuja lógica não é compreensível. Assim, são apontados 4 problemas centrais da explicabilidade: a opacidade, a estranheza, a imprevisibilidade e a justificação, destacando que tanto a

efetivação do princípio da transparência, uma vez que nem sempre é fácil ou, ainda, tangível, a explicação clara e a compreensão dos critérios e procedimentos utilizados no processamento de dados e na tomada de decisões.

Sobre esse fenômeno, Frank Pasquale em seu livro “The black box society. The secret algorithms that control Money and information”[15] pontua sobre a necessidade de um prévio conhecimento sobre o tema para possibilitar a efetiva regulação jurídica e, ainda, questiona até que ponto a ignorância algorítmica pode fazer parte de uma estratégia deliberada de algumas instituições conforme seus interesses privados.

Em contrapartida, ainda que a decisão guiada pelo algoritmo consiga ser tecnicamente explicada, muitas vezes é difícil tornar compreensível de modo simples as nuances técnicas que levaram àquela decisão, uma vez que os interessados nem sempre possuirão conhecimento técnico, o que, de igual modo, inviabilizaria a garantia do princípio da transparência, e, também do livre acesso, uma vez que a finalidade principal de prover a informação não foi efetivada.

Outra dificuldade relacionada à transparência pode surgir na falta de documentação clara e detalhada sobre o desenvolvimento, funcionamento e monitoramento dos algoritmos no chatbot, o que impede a análise crítica das decisões automatizadas e a identificação de possíveis falhas ou vieses. Assim, manter documentação completa e atualizada sobre todo o processo de desenvolvimento, funcionamento e monitoramento dos algoritmos é crucial para garantir a transparência e a revisão eficaz das decisões tomadas no âmbito do chatbot.

No entanto, vale pontuar que a LGPD estabelece uma possível exceção ao princípio da transparência quando este esbarrar na garantia do segredo comercial e industrial das instituições, conforme estabelecido no §1º do artigo 20. Frisa-se que tal restrição deve ser bem fundamentada e proporcional e, ainda assim, poderá ser passível de auditoria pela Autoridade Nacional de Proteção de Dados (ANPD) a fim de verificar a existência de práticas discriminatórias no tratamento automatizado de dados, conforme estipula o §2º do mesmo artigo.

opacidade quanto a justificação são problemas atuais que permeiam também decisões proferidas por seres humanos. Disponível em <link>). Acessado em 26 abri 2024.

[15] Pasquale, Frank. *The black box society. The secret algorithms that control money and information*. Cambridge: Harvard University Press, 2015. Disponível em <link>. Acessado em 26 abr. 2024.

Uma vez apresentados alguns aspectos e desafios relacionados ao cumprimento do art. 20 da LGPD, podemos elencar algumas dicas ao implementar um chatbot.

DICA

MEDIDAS PARA FACILITAR A CONFORMIDADE COM O ART.20 DA LGPD

- **Documentação.** Ter o registro de todo o processo de desenvolvimento do chatbot incluindo principalmente os algoritmos utilizados. Manter documentação completa e atualizada sobre o desenvolvimento, funcionamento e monitoramento dos algoritmos é crucial para a transparência e a revisão eficaz das decisões.
- **Ferramentas Adequadas**. Implementar ferramentas e tecnologias que facilitem o acesso, a análise e a visualização dos dados utilizados nos algoritmos é fundamental para a revisão rápida e eficiente das decisões. Isso inclui implementar mecanismos claros e acessíveis para que os usuários possam solicitar a revisão de decisões tomadas com base em seus dados.
- **Governança de Dados.** Estabelecer políticas e procedimentos internos de governança de dados, evidência de conformidade com as leis aplicáveis, revisões e testes periódicos e, ainda, assegurar medidas de segurança, qualidade e privacidade no chatbot.
- **Capacitação Equipes**. Investir na formação e treinamento de profissionais com expertise em inteligência artificial, proteção de dados e análise de algoritmos garante a expertise necessária para lidar com a revisão das decisões automatizadas.

Em conclusão a esse tópico é imprescindível entender que o artigo 20 da LGPD busca garantir aos indivíduos o direito de contestar decisões exclusivamente automatizadas que podem impactar seus interesses. No contexto dos chatbots, esse direito é essencial para garantir a proteção da privacidade, a transparência, a confiabilidade e a justiça nos processos decisórios baseados em dados. Preocupar-se desde o início da concepção do projeto do chatbot com a implementação de medidas adequadas, evidencia, por parte das instituições, a busca pelo uso responsável e ético da inteligência artificial, garantindo relações de confiança com os usuários e a ANPD e demais autoridades.

RESUMO

NESTE CAPÍTULO, VIMOS OS SEGUINTES PONTOS PRINCIPAIS:

- No item 3.1 foram entendidas algumas definições importantes relacionadas à LGPD: de dado pessoal, sua diferenciação com dado pessoal sensível, bases legais, o que pode ser considerado tratamento de dados pessoais e princípios.
- Já no item 3.2 foram estabelecidas as principais responsabilidades dos agentes de tratamentos de dados pessoais no decorrer de uma relação contratual e seus possíveis desdobramentos quando a ferramenta envolvida é um chatbot.
- Quanto ao item 3.3, foi abordado a fundo sobre o tratamento de dados pessoais em chatbots e os principais pontos a serem considerados em seu desenvolvimento, algumas medidas de segurança adequadas e questões relacionadas ao compartilhamento de dados pessoais e transferência internacional no contexto das relações contratuais entre agentes de tratamento.
- Por fim, no item 3.4 foi abordado sobre o tratamento automatizado de dados conforme os limites do art. 20 da LGPD e a preocupação com a garantia dos princípios da transparência e da não-discriminação. Aconselha-se a releitura deste tópico para todos os que pretendem utilizar um sistema automatizado que profira decisões sem a supervisão humana.

4. CONSIDERAÇÕES FINAIS

Neste Guia foram abordados os principais aspectos relacionados ao tratamento de dados pessoais em chatbots, uma ferramenta que tem se demonstrado muito útil e prática para a comunicação e gerenciamento de atividades em diversas instituições.

Preliminarmente, no Capítulo 2 foram estabelecidas as principais definições necessárias ao estudo deste Guia. Entendemos que um **chatbot** é um mecanismo automatizado de conversa, em que é possível a um usuário fazer perguntas e obter respostas geradas automaticamente, sejam elas supervisionadas por humanos, ou não. Entendemos, com definições simples, alguns conceitos importantes como **algoritmos, processamento de linguagem natural (PLN) e aprendizado de máquina/machine learning (ML).**

Conforme as fontes complementares anteriormente citadas, é importante avaliar se a tecnologia empregada em um chatbot aplica a noção de aprendizado de máquina, ou seja, se ela "aprende"

na medida em que interage com usuários, pois nesta hipótese os riscos da ferramenta podem ser maiores.

No item 2.2 foram estabelecidos alguns tipos de classificação de modelos de chatbots e os principais riscos relacionados à proteção de dados pessoais. Foi pontuado que antes de desenvolver um chatbot para atender a uma determinada função, é preciso previamente entender qual é a finalidade específica que se espera da ferramenta e o que é essencial para a realização da atividade. Assim, a partir dessa análise, é possível escolher o melhor modelo de chatbot a ser desenvolvido, sem que para isso a atividade seja exposta a um grau de risco desnecessário.

No Capítulo 3, foi iniciado o tema de proteção de dados pessoais em chatbots e as principais nuances a serem observadas pelas instituições visando a conformidade com a LGPD. Após a definição de conceitos básicos como dado pessoal, dado pessoal sensível, tratamento de dados pessoais, base legal e princípios no item 3.1, foram apontados no item 3.2 aspectos importantes de responsabilização dos agentes de tratamento na condição de controladores ou operadores.

No item 3.3 alguns tópicos inerentes ao tratamento de dados pessoais em chatbots foram levantados: dicas de etapas no desenvolvimento de um chatbot, medidas de segurança aplicáveis, como autenticação de identidade do usuário, criptografia, restrição de acesso, termos de sigilo, dentre outras, foram pontuadas. Foram levantados, também, aspectos centrais quando ao compartilhamento de dados pessoais em chatbots e transferência internacional de dados.

Por fim, no item 3.4 foi abordado sobre o tratamento automatizado de dados e a aplicação do art. 20 da LPGD. Quanto a este ponto, foi ressaltado que o direito à revisão da decisão mencionado no art. 20 abrange decisões exclusivamente baseadas em tratamento automatizado de dados, sem a intervenção humana no processo decisório e, ainda, que tal direito visa garantir a observância, em especial, dos princípios da transparência e não discriminação. Foram levantadas também, algumas dicas preciosas para auxiliar a conformidade das instituições com o art. 20.

O presente Guia destinou-se a oferecer diretrizes e boas práticas para instituições que estejam interessadas ou que já tenham implementado chatbots em seus processos internos e de relacionamento com o cliente. Buscou-se apresentar orientações à interpretação da LGPD, ressalvando-se futuros entendimentos de autoridades ou regulamentações específicas.

Este Guia é suscetível de constante mudança e atualização.

FGV DCI

DIRETORIA DE
CONTROLES INTERNOS