CONFORMIDADE DE *CHATBOTS* COM A LEI GERAL DE PROTEÇÃO DE DADOS - LGPD

The compliance of chatbots with the General Law of Data Protection - GLDP

Patrícia Peck Garrido Pinheiro[1]

ÁREA: Direito e Tecnologia. *Chatbots.*

RESUMO: O avanço tecnológico trouxe consigo um grande volume de dados que são utilizados cada vez mais pela Inteligência Artificial, dando suporte a aprendizagem de máquina. Esses dados privados do cidadão, cada vez mais expostos na rede mundial de computadores, precisam ser protegidos por legislação específica, como parte dos Direitos Humanos Fundamentais. O artigo se propõe a tratar do tema, mostrando suas consequências práticas quando são usados de forma indevida, utilizando-se do método dedutivo, baseado em pesquisa bibliográfica e referências a casos concretos.
PALAVRAS-CHAVE: Proteção de dados. Inteligência Artificial. *Chatbots.* Regulamentação. Direitos Humanos e tecnologia.

ABSTRACT: Abstract: The technological advance has brought a large volume of data increasingly used by Artificial Intelligence, supporting machine learning. These private citizen data, increasingly exposed on the World Wide Web, need to be protected by specific legislation as part of Fundamental Human Rights. The article aims to address the issue, showing the practical consequences when misused, using the deductive method based on bibliographic research and references to concrete cases.
KEYWORDS: Data protection. Artificial Intelligence. Chatbots. Regulation. Human Rights and technology.

[1] Advogada. Doutora em Direito Internacional pela Universidade de São Paulo – USP.

SUMÁRIO: 1. Introdução. 2. Para entender os *chatbots*: o que é a Inteligência Artificial? 3. *Chatbots* na prática. 4. *Chatbots* x LGPD. 5. Maus exemplos. 6. Conclusão. Referências.

1. INTRODUÇÃO

Vivemos em uma sociedade digital e conectada, em que a tecnologia intensifica, agiliza e democratiza as relações humanas. Nesse cenário, a aplicabilidade da Inteligência Artificial cresce cada dia mais, possibilitando a transformação de relações e procedimentos. Praticamente, é um assunto que remonta desde os anos 1950, mas que foi retomado e acelerado após os anos 2000 devido a fatores como: melhoria da qualidade dos algoritmos, poder de processamento e acesso a grandioso volume de bases de dados, capaz de apoiar na aprendizagem de máquina.

Por isso que a inovação digital deve ser a base da estratégia das organizações. A sociedade está ficando cada vez mais orientada por dados e o uso da Inteligência Artificial – IA- está no centro de todo o desenvolvimento tecnológico nos diversos setores da economia. É um novo pensar, com novas aplicações, que demandam suporte jurídico especializado para análise e viabilidade legal dos projetos, considerando o aumento do uso de chatbots, drones, *machine learning*, bases de dados, bem como para verificação de questões relacionadas à transparência e ética de algoritmos.

Projeções mostram que não deve demorar muito para a Inteligência Artificial fazer parte da nossa vida cotidiana em diferentes aspectos. Em breve, transporte, robôs domésticos, serviços, saúde, educação, entretenimento, comunidades de poucos recursos, segurança pública, emprego e local de trabalho serão espaços totalmente habilitados para IA.

Os desafios para os próximos 15 anos serão a criação de hardware seguro e confiável para seus diversos usos, seja de carros autônomos até robôs de saúde, para assim ganhar a confiança do público e dos consumidores. Com o avanço do uso desses recursos pelo mundo, grande parte dos países inicia o debate regulatório em torno dessa inovação tecnológica que tem grande potencial de mudar a forma como nos relacionamos e trabalhamos.

O ponto de partida da discussão gira em torno dos limites éticos das aplicações de Inteligência Artificial e alcança a questão de quais são os mecanismos de controle necessários para que a tão sonhada autonomia robótica não se vire contra o ser humano. Em geral, as regulamentações buscam tratar de alguns

pilares relacionados a 4 tipos de riscos relacionados à IA: riscos éticos, riscos de privacidade, riscos de cibersegurança e riscos de propriedade intelectual.

No caso do Brasil, tramita o PL 21/20[2] que busca regulamentar a Inteligência Artificial e que traz princípios inspirados nas iniciativas da OCDE e na UNESCO.

Sendo assim, como delimitar claramente os parâmetros que precisam ser seguidos por todos os setores da sociedade?

2. PARA ENTENDER OS CHATBOTS: O QUE É A INTELIGÊNCIA ARTIFICIAL ?

De acordo com Barthe (2017), a terminologia foi criada por John McCarthy e definida por Marvin Lee Minsky do seguinte modo:

> [..] a construção de programas de computador que se engajam em tarefas que são, por enquanto, realizadas a partir de mais satisfatoriamente por seres humanos, porque eles exigem processos mentais de alto nível, tais como: aprendizagem perceptiva, organização da memória e raciocínio crítico[3].

O estudioso Adriano Mussa (2020) define a Inteligência Artificial como o "[...] uso de modelos estatísticos ou matemáticos em aplicações específicas para predição de resultados, buscando sempre a máxima acurácia e robustez possíveis[4]".

A pesquisadora Elaine Rich sintetiza a IA no seguinte enunciado: "Uma área de pesquisa que investiga formas de habilitar o computador a realizar tarefas nas quais, até o momento, o ser humano tem um melhor desempenho"[5].

---

[2] O PL 21/2020, de autoria do deputado federal Eduardo Bismarck, estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil; e dá outras providências. No momento o projeto aguarda análise do Senado Federal. Disponível em: <https://www.camara.leg.br/propostas-legislativas/2236340>. Inclusive, neste ano foi instaurada uma comissão de juristas responsável por subsidiar a elaboração de substitutivo sobre inteligência artificial no Brasil. Disponível em: <https://www12.senado.leg.br/noticias/materias/2022/03/24/comissao-de-juristas-comecara-a-analisar-projetos-sobre-inteligencia-artificial>. Vale destacar os princípios da Unesco (https://pt.unesco.org/courier/2018-3/em-direcao-um-codigo-etica-global-pesquisa-em-inteligencia-artificial) e da OCDE (https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449).

[3] BARTHE, Emmanuel. **Intelligence artificielle en droit**: derrière la "hype", la réalité. Un blog pour l'information juridique, nov., 2017. Disponível em: <http://www.precisement.org/blog/Intelligence-artificielle-en-droit-derriere-la-hype-la-realite.html#definir>.

[4] MUSSA, Adriano**. Inteligência Artificial** – mitos e verdades: as reais oportunidades de criação de valor nos negócios e os impactos no futuro do trabalho. São Paulo: Saint Paul, 2020. p. 65

[5] RICH, Elaine **Artificial Intelligence**. New York: McGraw Hill Higher Education, 1991.

Deste compilado de conceituações, podemos inferir que a IA é um sistema/algoritmo (software) cuja meta é *entender* e *construir* sistemas inteligentes, de forma que as máquinas inteligentes são desenvolvidas sob as seguintes motivações[6]:

- Melhor compreensão sobre nós (humanos);
- As máquinas inteligentes se mostram bastante úteis e interessantes quando aplicadas de maneira direcionada;
- A capacidade de desenvolvimento das IAs transcende as barreiras biológicas, podendo trazer avanços inimagináveis ao desenvolvimento humano.

Em suma, um sistema inteligente é capaz de[7]:

- Aprender por experiência;
- Utilizar o conhecimento adquirido;
- Solucionar problemas;
- Reagir perante uma nova situação – de modo ágil;
- Determinar o que é ou não importante;
- Racionar/pensar;
- Processar e manipular dados;
- Imaginar e criar dentro de um contexto de dados.

No caso, os *chatbots* são ferramentas de comunicação automatizadas, que utilizam IA para simular uma interação nos atendimentos *on line* das empresas. Normalmente programado para reproduzir uma conversa humana num *chat.* A vantagem desse sistema é automatizar tarefas que se repetem constantemente (como dúvidas frequentes), na forma de diálogo entre o usuário e um "robô".

3. *CHATBOTS* NA PRÁTICA

Para imaginar o avanço dessas ferramentas, uma pesquisa realizada pela MarketsandMarkets[8] revela que o mercado de chatbots é bastante promissor e

[6] BARANAUKAS, José Augusto. **Histórico e Aplicações de Inteligência Artificial**. [notas de aula]. 2020.

[7] Id.

[8] Disponível em: < https://www.marketsandmarkets.com/Market-Reports/conversational-systems-market-232318863.html>.

deverá crescer 30% ao ano até 2024. Segundo o levantamento, que ouviu 1.235 consumidores, 69% dos entrevistados estão satisfeitos com o uso desses "robôs" nas interações dos atendimentos.

De acordo com a Pesquisa Panorama Mobile Time - Mapa do Ecossistema Brasileiro de *Bots* - Agosto de 2021[9], em um ano dobrou a quantidade de *bots* produzidos até hoje no Brasil, passando de 101 mil para 216 mil. O tráfego mensal de mensagens trocadas por esses *bots* cresceu 27%, subindo de 2,2 bilhões para 2,8 bilhões. Já a quantidade de robôs de conversação em atividade no Brasil praticamente dobrou entre 2020 e 2021, passando de 24 mil para 47 mil. Em média, cada um desses robôs conversa com 5,5 mil pessoas diferentes por mês e registra um tráfego mensal de 58 mil mensagens.

Algumas instituições já fazem uso de algum *chatbot* para orientação e atendimento. Um exemplo prático é o da "Privy"[10] (*chatbot* exclusivo), que tem o objetivo de responder dúvidas sobre a Lei Geral de Proteção de Dados Pessoais (LGPD) com velocidade e precisão. O projeto envolve a participação de uma equipe multidisciplinar tanto de cientista de dados, programadores, como estagiários de direito que têm a oportunidade de aprender como programar e treinar um *chatbot*.

Assim, os estudantes têm a oportunidade de atuar com uma equipe multidisciplinar especializada em ciências de dados. Esse exercício traz uma visualização muito importante para esses profissionais que estão se preparando para serem advogados do Direito Digital. A formação atual exige essa expertise de conhecer de forma mais aprofundada tanto o direito, quanto a tecnologia.

4. *CHATBOTS* X LGPD

Todos os assistentes virtuais, de qualquer instituição, seja ela pública ou privada, além de seguirem uma conduta ética e transparente, precisam estar em conformidade com a regulamentação de proteção de dados pessoais. Toda interface com tratamento de dados pessoais de titulares precisa informar isso.

Não importa se é a recepção de um prédio, uma página na web, um telefonema atendido por uma URA, ou um *chatbot.* A lei exige que as instituições divulguem os contatos do seu encarregado pelo tratamento de dados, conhecido como DPO (*Data Protection Officer*). Isso deve ser feito preferencialmente no

[9] Disponível em: <https://www.mobiletime.com.br/pesquisas/mapa-do-ecossistema-brasileiro-de-bots-2021/>.

[10] Privy+ é o *chatbot* do escritório Peck Advogados acessível na página https://www.peckadv.com.br/

sítio eletrônico da empresa, mas se o seu principal canal de contato com os consumidores for um *bot*, é recomendável que essa informação esteja disponível no fluxo de conversa com o robô.

Também não é demais lembrar que toda interação com o *bot* é uma evidência. Fica registrada ali a conformidade ou a desconformidade com a lei, sendo inclusive uma prova que pode levar a empresa a sofrer penalidades.

Novamente de acordo com a edição de 2022 do Mapa do Ecossistema Brasileiro de Bots[11], 53% dos desenvolvedores de robôs de conversação que atuam no Brasil afirmam que seus *bots* estão adequados à LGPD. Apenas 3% informam que cerca de metade está aderente à lei; outros 3% dizem que poucos estão; e 6% não souberam responder.

Em uma sociedade tecnológica que está caminhando para o maior uso da inteligência artificial, é essencial, do ponto de vista ético, que o ser humano seja sempre informado e tenha plena ciência de quando está interagindo com um robô. O que significa ter que haver uma declaração que diferencie o perfil autêntico (atribuído a uma conta humana) de um que não seja.

Além disso, o atendimento virtual precisa explicar sobre a política de privacidade da instituição, sobre os canais de atendimento e confirmar se a identidade da pessoa que busca a interação com os aplicativos de comunicação é a correta. Por exemplo, já vimos casos de atendimentos de *chatbots* de laboratórios que queriam confirmar agendamento de exames, mas mandaram mensagem para a pessoa errada. Pode-se ocasionar ali uma exposição de um dado pessoal sensível que está relacionado à saúde.

O *bot*, caso capte dados pessoais de seus usuários, precisa estar em conformidade com a LGPD e atender requisitos de privacidade e segurança. E seu algoritmo deve buscar a transparência e a ética, e ser capaz, entre outras ações, de deixar claro de que se trata de um *bot;* explicar os motivos dos dados serem coletados e verificar a identidade da pessoa antes de encaminhar dados sensíveis, como resultado de exame.

5. MAUS EXEMPLOS

Uma abordagem falha do robô pode causar problemas. Por exemplo, se um *bot* de um laboratório clínico entrar em contato com um suposto paciente para informar que o resultado do exame poderá ser acessado em uma determinada

[11] Disponível em: <https://www.mobiletime.com.br/pesquisas/mapa-do-ecossistema-brasileiro-de-bots-2021/>.

plataforma, mas a pessoa escreve que não fez nenhum exame. O *bot* desconsidera e continua a conversa. No fim, ainda pede para responder uma pesquisa de opinião.

Em outro exemplo de desconformidade, um cliente manda mensagem pedindo o resultado de seus exames e informa nome e o Cadastro de Pessoa Física – CPF perante a Receita Federal. O robô já envia um arquivo PDF com os resultados sem verificar a identidade. O correto seria o *bot* validar a identidade da pessoa.

O *bot* tem que estar treinado para situações em que liga para a pessoa errada. Não podemos apresentar dado pessoal sensível para outra pessoa que não é proprietária desse dado.

Outro aspecto muito importante envolve a ética algorítmica utilizada nessas plataformas, que pode ser identificada em uma auditoria. Entre os pontos questionados, é possível detectar se o algoritmo:

- possui viés estatístico;
- possui viés social que reflita vantagens sistemáticas para um ou mais grupos e desvantagem aos demais;
- é transparente na arquitetura;
- é transparente quanto aos critérios e métricas para a tomada de decisão automatizada.

São meios de garantir a transparência e a não discriminação do bot. É importante que ele passe uma comunicação clara, transparente e acessível de quais dados estão sendo coletados. Logs têm que ser bem guardados, assim como a tabela de temporalidade de guarda. E são necessários cuidados no treinamento do motor para não ter frases machistas, racistas e discriminatórias. É o *explainable* AI, ou seja, o princípio de explicabilidade do algoritmo.

Em linhas gerais, o que se busca com a regulação dos dados pessoais, no Brasil e demais países, é assegurar um manuseio ético, justo e ponderado dos dados em tratamento, de modo que, em relação às IAs, prevaleça a busca de garantia dos seguintes princípios norteadores:

a) **Respeito à autonomia humana:** sistemas inteligentes devem respeitar em todos os momentos a autonomia e os direitos fundamentais das pes-

soas. Portanto, o design e programação devem respeitar a vida e os direitos humanos sem qualquer tipo de discriminação.

b) Transparência: no caso de sistemas de IA, a transparência diz respeito principalmente à explicabilidade e rastreabilidade dos referidos sistemas. Esses dispositivos foram desenvolvidos para tomar decisões automaticamente com base em diferentes cálculos e projeções, e a possibilidade de rastrear o tempo todo o raciocínio seguido pelo sistema e explicar as consequências alcançadas. Especificamente, deve ser possível rastrear o conjunto de dados usado no raciocínio, a operação do algoritmo e as etapas seguidas para alcançar resultados. Todo esse processo também deve ser explicado a partir das visões técnicas de programação e design humano. O design e o uso de tecnologia imprevisível são uma combinação incompatível com a defesa da autonomia humana. É absolutamente necessário que a atividade de todos esses dispositivos seja fácil de entender e acessar.

c) Responsabilidade e prestação de contas: estreitamente relacionados ao princípio anterior, o design e o uso de sistemas inteligentes devem ser precedidos por uma clara alocação de responsabilidades por possíveis danos, e danos que isso possa causar. A alegada autonomia desses sistemas não pode servir de pretexto para a diluição de responsabilidades. Ao contrário, será necessário incluir os mecanismos apropriados (auditoria, relatório de erros, multas etc.) para garantir que as responsabilidades e obrigações relacionadas com a operação desses sistemas estejam bem definidas.

d) Robustez e segurança: a confiabilidade da IA exige que algoritmos sejam seguros, confiáveis e robustos o suficiente para operar com precisão e segurança, e resolver erros ou inconsistências durante todas as fases do ciclo de vida útil dos dispositivos. Este princípio também exige que os sistemas sejam projetados e desenvolvidos considerando a possibilidade de ataques cibernéticos e falhas técnicas.

e) Justiça e não discriminação: a concepção desses sistemas deve contar com a participação das partes interessadas e relacionadas com cada aplicativo que forneceu IA. Além disso, esses dispositivos devem garantir um

emprego justo dos dados disponíveis para evitar possíveis discriminações ou até distorções nos preços, afetando o equilíbrio do mercado[12].

6. CONCLUSÃO

Com efeito, um dos grandes embates e desafios deste campo da ciência jurídica é desenvolver uma legislação voltada à IA que consiga harmonizar as intenções mercadológicas e os Direitos Humanos fundamentais.

Para o Brasil assumir a dianteira para liderar a pauta de inovação, precisa tomar mais proveito da experiência internacional e aplicar ferramentas mais dinâmicas que permitam maior interação público-privada, com uso de recursos que envolvam não só a regulamentação, mas também atividades de corregulação e autorregulação para o desenvolvimento sustentável da IA, ou seja, de *hard law* (lei, decreto, portaria etc.) e de *soft law* (códigos de conduta, melhores práticas, frameworks, guias etc.).

REFERÊNCIAS

BARANAUKAS, José Augusto. **Histórico e Aplicações de Inteligência Artificial**. [notas de aula]. 2020.

BARTHE, Emmanuel. Intelligence artificielle en droit: derrière la "hype", la réalité. **Un blog pour l'information juridique,** nov., 2017. Disponível em: <http://www.precisement.org/blog/Intelligence-artificielle-en-droit-derriere-la-hype-la-realite.html#definir>. Acesso em jul-22.

GARCÍA, Sergio Marín. **Ética e** inteligência artificial. **Cátedra Caixabank de Responsabilidad Social Corporativa**, Cad. nº 42, set. 2019.

MUSSA, Adriano**. Inteligência Artificial** – mitos e verdades: as reais oportunidades de criação de valor nos negócios e os impactos no futuro do trabalho. São Paulo: Saint Paul, 2020.

[12] GARCÍA, Sergio Marín. **Ética e** inteligência artificial. **Cátedra Caixabank de Responsabilidad Social Corporativa,** Cad. nº 42, set. 2019. p. 18 e 19.

RICH, Elaine **Artificial Intelligence**. New York: McGraw Hill Higher Education, 1991.

Submissão: 31.maio.2022
Aprovação: 31.julho.2022