IAs generativas personalizadas e a “pessoa algorÃtmica”

Personalização é uma peça central quando se pensa na expansão da internet, de produtos e serviços digitais e, especialmente, no avanço da inteligência artificial (IA). E as razões da constatação desse fato são das mais variadas: comodidade, filtragem de acessos, rapidez para encontrar o que se busca, sugestões de bens de consumo novos baseados em interesses externalizados em buscas anteriores e no comportamento *online*, economia de tempo nas tarefas cotidianas e maior produtividade e assim por diante. Não seria ótimo se tivéssemos nossa IA pessoal, capaz de performar diversas tarefas, como classificar por relevância e responder *e-mails* ou programar, convidar amigos e adquirir itens para uma

Essa é a promessa de um futuro não muito distante. Há alguns dias, o

Google anunciou uma série de novas funcionalidades no Bard, sua inteligência artificial generativa e maior concorrente do ChatGPT. Uma delas em especial chama atenção se olharmos pela lente da proteção de dados pessoais: a capacidade de conexão do Bard com aplicativos e outros serviços do próprio Google que já são utilizados por nós, consumidores. Isso significa que nossas informações hoje distribuídas entre Gmail, Drive, Docs, Maps, YouTube, entre outros, podem ser recrutadas a nosso comando para que o Bard faça seu trabalho. Trata-se do "Bard Extensions" que, segundo a próprio Google, é uma forma inteiramente nova de *"interagir e colaborar com o Bard"* [1].

Alguns usos são apontados no blog do Google e ilustram como a integração funciona. É possível pedir ao Bard que verifique, dentro de um determinado conjunto de e-mails trocados com pessoas específicas, datas que atenderiam a todas as agendas para que uma reunião seja marcada. Outra situação é a solicitação para que o Bard vasculhe no Google Drive a versão mais recente do currículo do usuário, que o traduza para outro idioma e que faça um breve resumo das qualificações levando em consideração o perfil do empregador em potencial.

A integração também contempla o Google Fotos onde o sistema pode acessar, classificar e analisar não apenas as imagens, mas também os metadados, que carregam em si outro conjunto de informações pessoais. Isso sem mencionar as imagens de terceiros, eventualmente de crianças e adolescentes que por si só demandam outra camada de proteção. Para aqueles que usam o Google Viagens, a promessa é funcionar como um assistente pessoal cruzando, por exemplo, passagens já compradas com as melhores ofertas de hotéis, contratação de translado e identificação de eventos como peças e exposições nos destinos.

Essa nova ferramenta tem como função principal algo… diferente: interessante, tentador, ou, melhor: inebriante, como diria o filósofo sul-coreano Byung-Chul [2]. Isso porque o seu objetivo não é agir somente sobre dados disponíveis na internet, mas em dados pessoais *online* mais "reservados", mas que são constantes da sua grande família de aplicativos. Ou seja, diferentemente dos outros modelos de IAs generativas, o Bard, com esses acessos, saberá mais ainda sobre o seu usuário, tornando a ferramenta, do ponto de vista utilitário, muito melhor para a realização de tarefas do cotidiano. É um passo, sem dúvidas, à personalização da IA.

Porém, antes que estejamos por completo inebriados convém compreender o que essa integração significa em termos de proteção de dados pessoais. A propósito, uma questão antecipada pelo próprio Google ao afirmar que (1) os dados pessoais dos consumidores do "Bard Extensions" não serão usados como fonte de treinamento do sistema, (2) não serão submetidos a revisores humanos, e (3) não serão tomados como insumo para fins de publicidade direcionada.

Todavia, nas políticas atualizadas dessa IA, de 18 de setembro de 2023, ainda persiste um conselho que o próprio Google nos dá sem maiores especificidades de que isso não se aplicaria a suas novas extensões: *"por favor, não insira informações confidenciais em suas conversas no Bard ou qualquer dado que você não gostaria que um revisor visse ou que o Google usasse para melhorar nossos produtos, serviços e tecnologias de aprendizado de máquina"* [3].

Será que esses três pontos são suficientes para garantir o direito fundamental à proteção dos dados pessoais dos consumidores? É o que analisamos a seguir.

É sabido que o funcionamento dos sistemas de inteligência artificial generativa depende de uma grande quantidade de dados. Os modelos são treinados justamente com base em dados, e nesse quesito quantidade e qualidade impactam diretamente nos resultados obtidos. Cabe lembrar que o treinamento é apenas uma das atividades de tratamento de dados pessoais que um sistema de IA, a exemplo do Bard, realiza. De acordo com o artigo 5º, X da Lei Geral de Proteção de Dados Pessoais (LGPD), o tratamento engloba toda operação que envolve dados pessoais, a exemplo de: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Logo, afirmar que os dados dos usuários não serão usados para fins de treinamento não significa que outras formas de tratamento não estarão em curso. Inicialmente seria necessário compreender o conjunto de operações que ocorrem fora da etapa de treinamento do sistema. Afinal, para além de treinar a inteligência artificial, há a entrega efetiva dos resultados prometidos de acordo com a demanda do usuário. A título de ilustração, a integração entre o Bard e o Gmail aponta para o envolvimento de dados pessoais de terceiros na medida em que as solicitações sejam relacionadas à identificação de e-mails trocados entre diferentes titulares. Situação capaz de ensejar violações não apenas relacionadas a dados pessoais, mas também a dados pessoais sensíveis, uma vez que o conteúdo dos e-mails é o mais variado possível.

No que se refere à não submissão das informações tratadas a revisores humanos, a princípio não denota maior relevância para fins da tutela à proteção de dados. Aqui parece se estar diante da lógica já ultrapassada segundo a qual o direito à privacidade se estruturava em torno da pessoa-informação-segredo, e não diante da noção de controle do fluxo dos próprios dados pessoais [4]. Ademais, não fica claro qual seria a finalidade da revisão para que se pudesse avaliar o real impacto sobre a privacidade dos usuários de ter ou não revisores humanos.

Por fim, o terceiro e último ponto antecipado por ocasião do lançamento do "Bard Extensions": a não utilização dos dados pessoais dos usuários para fins de publicidade. Trata-se de um tema especialmente sensível para o Google. Não apenas pela representatividade do negócio de publicidade na receita total da empresa, mas também pela forma como se deu seu desenvolvimento, avançando cada vez mais sobre informações pessoais dos usuários. O que acabou criando uma constante tensão entre a empresa e os órgãos de fiscalização voltados para a proteção da privacidade e dos dados pessoais.

A prática de monitoramento de conteúdo de e-mail, por exemplo, já havia levado a empresa à justiça nos EUA: em setembro de 2015, no caso Mattera *vs* Google [5], não usuários de contas G-mails que trocavam e-mails com usuários de contas G-mails foram ao tribunal distrital do norte do estado da Califórnia alegando violação do Federal Electronic Communications Privacy Act e do California Invasion of Privacy Act. Em junho de 2017 o Google anunciou que encerraria a atividade monitoramento de e-mails dos usuários das contas gratuitas do G-mail para fins de envio de publicidade. O anúncio foi publicado no blog oficial da empresa e afirmava que os mais de 1,2 bilhão de consumidores do G-mail continuariam recebendo publicidade personalizada, mas que a fonte de informação para os anúncios deixaria de ser o conteúdo obtido com a prática do escaneamento [6].

A lembrança desse caso se presta a reforçar a noção de que o monitoramento de e-mails é apenas uma maneira de coletar dados pessoais. No entanto, a não utilização para fins de publicidade não exclui necessariamente outras formas de tratamento diversas, nem que as informações pessoais serão utilizadas para outras finalidades – nem sempre informadas, nem sempre compatíveis com a finalidade originária. Quer dizer tão somente que os dados não serão usados para fins publicitários.

Em uma primeira análise, podemos apontar que a integração pioneira de um produto baseado em Grandes Modelos de Linguagem (LLM) com aplicativos repletos de dados pessoais do próprio usuário e de terceiros representa um agravamento na eventualidade de tratamento irregular. De acordo com o artigo 44, da LGPD, isso pode ocorrer tanto pela inobservância da legislação, quanto pela desconformidade no grau de segurança esperada pelo usuário.

Todas estas questões que têm, como pano de fundo, uma pretensa personalização (agora também) de práticas e técnicas, como a IA, podem ter como consequência o agravamento da vulnerabilidade digital dos consumidores. Ela representa uma forma complexa de vulnerabilidade, uma vez que, além das suas características distintas que lhe conferem contornos específicos, incorpora as vulnerabilidades tradicionais bem conhecidas dos consumidores, que são transportadas e codificadas no ambiente *online* . Segundo Canto, a vulnerabilidade típica das relações de consumo se transforma com o advento das novas tecnologias, o que amplia a fragilidade do consumidor [7].

Podemos então conceituar a vulnerabilidade digital como aquela que *"descreve um estado universal de indefesa e suscetibilidade a (exploração de) desequilíbrios de poder que são resultado da crescente automação do comércio, da datificação das relações consumidor-fornecedor e da própria arquitetura dos mercados digitais"*, sendo multimodal, pois refere-se às dinâmicas, práticas e contratos tecnológicos, à complexidade de produtos e serviços, a qualidades ou circunstâncias específicas dos consumidores descobertas em dados pessoais que são exploradas para fins comerciais. Assim, *"a vulnerabilidade é sobre o poder ou a capacidade dos atores comerciais de afetar as decisões, desejos e comportamentos do consumidor de maneira que o consumidor, tudo considerado, não tolera, mas também não está em posição de impedir"* [8].

Personalização e acesso a dados pessoais e seu respectivo tratamento, combinados com o desenvolvimento de poderosas ferramentas tecnológicas, como a IA generativa, que traz a promessa de maior conforto e produtividade, significa maior vulnerabilidade dos consumidores por diferentes razões, mas aqui gostaríamos de destacar um aspecto que merece umas linhas iniciais de pensamento. Falamos da nova catividade digital dos contratos e da dependência: na medida em que uma plataforma central se consolida na corrida por uma tecnologia como o Bard, integrando-a a seus serviços digitais que já são dominantes no mercado, sua posição de poder (*Machtposition*) tende a se solidificar, representando dificuldades a consumidores que, eventualmente, queiram trocar de fornecedor ou que queiram discordar da máquina.

Isso porque a troca de fornecedor tem custos (monetários, pessoais ou outros): se não operacionalizada a portabilidade de dados pessoais em diversos âmbitos, ao se deletar uma conta de e-mail, todos as suas comunicações, fotos e arquivos serão deletados ou, pelo menos, não se terá mais acesso sobre eles. No Drive, todos os arquivos correspondentes assim o serão. E assim por diante. Se já estamos imersos nos serviços Google, dificilmente sairemos deles, considerando ainda que mais e mais camadas de "facilidades" são desenvolvidas, como o "Extensions". Em termos contratuais, isso significa um aprofundamento dos contratos cativos de longa duração, que parecem ser a regra no mundo digital, não a exceção. Do lado prático, conhece-se o fenômeno como "efeito *lock in*", significando justamente o aprisionamento do consumidor a um determinado fornecedor, resultando em maiores níveis de personalização por conta da duração prolongada no tempo da coleta e tratamento de dados pessoais que acompanha, indissociavelmente, a fruição de serviços digitais.

Mas dependência também poderá ser vista pelo prisma da hiperconfiança, no sentido de que a pessoa fica dependente de sistemas inteligentes para tomar decisões, de modo que, com o passar do tempo, fica-se, de fato, como um "selo humano" de decisões de máquinas. Em outros termos, consumidores poderão se guiar progressivamente pelo que o Google decide e mostra em termos de conteúdo, já que "ele me conhece" e tem sistemas avançados de análises de dados ditos mais objetivos, imparciais e mais atentos às necessidades do titular. Daqui também poderemos compreender as alucinações, os resultados inventados, discriminatórios, preconceituosos, injustos ou abusivos, ou mesmo errados e totalmente inventados que podem ser seus *outputs*.

O futuro da internet não sabemos. Mas é possível percebermos que – assim como o mercado automatizou diversas facetas – estamos, agora nós (mas por intermédio do mercado!), automatizando (e moldando) nossas relações, nossa capacidade decisória, nossa comunicação digital e, em última análise, nosso comportamento e nós mesmos [9] – o que demandará uma apreciação cuidadosa do ordenamento jurídico, como, por exemplo, a análise da má-fé aplicada ao comportamento de agentes puramente informacionais em alguns casos [10].

[1]Google AI. Bard: um grande modelo de linguagem. Disponível em: https://support.google.com/bard/answer/13594961?hl=en. Acesso em: 21/09/2023.

[2] HAN, Byung-Chul. *No enxame:* perspectivas do digital. Petrópolis: Editora Vozes, 2013. p. 9.

[3]Suporte do Google Bard. Disponível em: https://support.google.com/bard/answer/13594961?hl=en. Acesso em 21/09/2023.

4 DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Saraiva Educação, 2022.p. 41.

[5] Matera v. Google Inc., 15-CV-04062-LHK, 2016 WL 6769137 (Câmara Distrital dos Estados Unidos para o Distrito Sul da Califórnia, 8 de dezembro de 2016)

[6] Google. *G Suite ganha força no mercado corporativo*: G Suites Gmail e consumidor Gmail para se alinharem mais de perto. Blog Google, 01 de junho de 2023. Disponível em: < https://blog.google/products/gmail/g-suite-gains-traction-in-the-enterprise-g-suites-gmail-and-consumer-gmail-to-more-closely-align/>. Acesso em: 05 de outubro de 2023.

[7] CANTO, Rodrigo Eidelvein. *A vulnerabilidade dos consumidores no comércio eletrônico*: reconstrução da confiança na atualização do Código de Defesa do Consumidor. São Paulo: Revista dos Tribunais, 2015. p. 91.

[8] HELBERGER, N.; SAX, M.; STRYCHARZ, J.; MICKLITZ, H.â?•W. Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability. *Journal of Consumer Policy*, nov. 2021. DOI: https://doi.org/10.1007/s10603-021-09500-5. p. 9.

[9] GAL, Michal S.; ELKIN-KOREN, Niva. Algorithmic Consumers. Harvard Journal of Law &

Technology, v. 30, n. 2, Primavera 2017, 45 p.

[10] Veja, nesse sentido, a título de ilustração: “CONSUMIDOR. BANCO. COBRANÇA INDEVIDA. DÍVIDA INEXISTENTE E PAGA. REPETIÇÃO DO INDÉBITO. FORMA SIMPLES. ARTIGO 42, § ÚNICO DO CDC. ART. 940 DO CÓDIGO CIVIL. MÁ-FÉ NÃO COMPROVADA. INTELIGÊNCIA ARTIFICIAL. PRECEDENTES DO STJ. 1. "A aplicação do art. 42, parágrafo único, do Código de Defesa do Consumidor somente é justificável quando ficarem configuradas tanto a cobrança indevida quanto a má-fé do credor fornecedor do serviço. Precedentes do STJ" (AgRg no REsp 1200821/RJ, Relator Ministro JOÃO OTÁVIO DE NORONHA, TERCEIRA TURMA, julgado em 10/02/2015, DJe 13/02/2015.). 2. Para que haja a devolução em dobro do indébito, é necessária a comprovação de três requisitos, conforme o parágrafo único do artigo 42 do CDC, a saber: 1) que a cobrança realizada tenha sido indevida; 2) que haja o pagamento indevido pelo consumidor; e 3) que haja engano injustificável ou má-fé. Mutatis mutandis, a mesma exigência impõe-se para a repetição ou para a indenização prevista no art. 940 do Código Civil. 3. A má-fé é inerente à atitude humana de quem age com a intenção deliberada de enriquecimento ilícito ao cobrar o que já foi pago, ao receber o que foi cobrado e ao cobrar o que não era devido, sem qualquer engano ou erro justificável. 4. Para a devolução em dobro, não basta a cobrança indevida. As instituições financeiras, conceito que compreende bancos e, também, companhias que administram operações de cartões de crédito, conhecidas como bandeiras, operam com inteligência artificial, a chamada 4ª Revolução Industrial, que é caracterizada pela fusão de tecnologias que puseram em xeque as esferas física, digital e biológica. Não há como se imputar má-fé às cobranças feitas por sistemas computacionais, por robôs eletrônicos. 5. Há que se repensar conceitos que não poderão receber dos juristas as antigas soluções impostas pelo Direito Romano ao vendedor de balcão, com caderneta de apontamentos pessoais dos seus fregueses, contemporânea da 1ª Revolução Industrial, a era da máquina movida a vapor. 6. As inconsistências do emprego de inteligência artificial não podem ser punidas com o rótulo da má-fé, atributo exclusivamente humano, ínsito a quem anota, naquela mencionada caderneta, uma compra que não foi feita ou uma dívida que já foi paga, para dobrar, fraudulentamente, o lucro no fim do mês. 7. Sem os requisitos legais, a devolução do indébito deve ocorrer de forma simples. 8. Recurso conhecido e parcialmente provido. (TJ-DF 07150148120188070001 DF 0715014-81.2018.8.07.0001, Relator: EUSTÁQUIO DE CASTRO, Data de Julgamento: 14/03/2019, 8ª Turma Cível, Data de Publicação: Publicado no DJE : 06/05/2019 . Pág.: Sem Página Cadastrada.)