Os algoritmos e a transparência no tratamento de dados pessoais no contexto da internet: uma análise luso-brasileira

Camila Schwonke Zanatta[1]

Resumo: O artigo analisa o princípio da transparência no tratamento de dados pessoais no ambiente digital, com enfoque nas legislações brasileira (LGPD) e europeia (RGPD). Através de uma metodologia qualitativa e analítico-comparativa, explora os desafios da coleta automatizada, o uso de algoritmos e a opacidade das decisões baseadas em inteligência artificial. Defende a transparência como requisito essencial à autodeterminação informativa. Propõe a explicabilidade, auditoria e educação digital como formas de mitigar riscos, reforçando o papel da transparência como eixo estruturante da proteção de dados pessoais.

Palavras-chave: Transparência; Algoritmo; Dados Pessoais; LGPD; RGPD;

Abstract: This article analyzes the principle of transparency in personal data processing within the digital environment, with a focus on Brazilian (LGPD) and European (GDPR) legislation. Using a qualitative and analytical-comparative methodology, it explores the challenges of automated data collection, algorithmic use, and the opacity of artificial intelligence-based decisions. Transparency is defended as an essential requirement for informational self-determination. It proposes explainability, auditing, and digital education as means to mitigate risks, reinforcing transparency's role as a structural pillar of personal data protection.

---

[1] Mestre e Doutoranda em Direito e Ciência Jurídica na Faculdade de Direito da Universidade de Lisboa. camilaszanatta@gmail.com

Keywords: Transparency; Algorithm; Personal Data; LGPD; GDPR;

Introdução

A transparência no tratamento de dados pessoais obtidos na internet constitui princípio fundamental do Direito Digital contemporâneo. Em um cenário marcado pela natureza transfronteiriça e pelo anonimato característico da internet, compreender de que forma as informações dos usuários são tratadas, processadas e compartilhadas torna-se requisito essencial para a efetividade da autodeterminação informativa[2], direito intrinsecamente ligado à dignidade da pessoa humana.

No plano normativo, tanto o Regulamento Geral de Proteção de Dados (RGPD), aplicável em Portugal e na União Europeia, e a Lei Geral de Proteção de Dados (LGPD) no Brasil, consagram a transparência como princípio estruturante do direito de proteção de dados. Essas normas impõem o dever de informação e explicabilidade aos agentes de tratamento, de modo que eventuais decisões automatizadas ou o uso de algoritmos para perfilamento não resultem em discriminação injustificada ou violação de direitos individuais.

Entretanto, a opacidade que caracteriza muitos sistemas algorítmicos, somada à complexidade técnica das soluções de Inteligência Artificial (IA), desafia a concretização desse princípio. Em especial, há divergências relevantes entre o RGPD e a LGPD quanto ao alcance da obrigação de transparência, ao tratamento das decisões exclusivamente automatizadas e aos mecanismos de fiscalização e sanção.

Nesse contexto emerge uma questão: em que medida o princípio da transparência, tal como disciplinado no RGPD e na LGPD, é capaz de mitigar os riscos decorrentes da opacidade algorítmica, e quais são as implicações práticas das diferenças regulatórias entre Portugal/União Europeia e Brasil para a proteção de dados pessoais no ambiente digital?

---

[2] Artigo 2.º, inciso II, da LGPD.

Para tanto, adota-se uma abordagem qualitativa, de natureza exploratória e analítico-comparativa, voltada à compreensão das convergências e divergências entre o regime europeu e o brasileiro de proteção de dados pessoais partindo de uma revisão bibliográfica e normativa, abrangendo legislação, doutrina especializada, pareceres e documentos técnicos emitidos por autoridades de proteção de dados. A análise restringe-se ao tratamento de dados pessoais no contexto da internet, com ênfase nas práticas algorítmicas e nos processos de tomada de decisão automatizada.

1. A Noção de Transparência no Tratamento de Dados Pessoais

a. Origem e evolução do princípio da transparência

Inicialmente, há de se falar que a Constituição Portuguesa de 1976 foi uma das primeiras constituições do mundo a tratar da questão da proteção dos dados pessoais. Esta previa no artigo 35.º sob a epígrafe "Utilização da Informática" o direito de todos os cidadãos de tomar conhecimento do que constar dos registos mecanográficos a seu respeito e do fim a que se destinam as suas informações, podendo exigir a sua retificação dos dados e atualização[3]. Não permitia o uso da informática para o tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se tratasse do tratamento de dados não identificáveis para fins estatísticos[4].

O artigo 35.º na redação atual, que mantém a mesma epígrafe, prevê o direito de acesso aos dados informatizados que lhe digam respeito, direito de retificação e atualização, o direito a conhecer a finalidade a que se destinam[5]. Também veda a utilização da informática

[3] Versão inicial do artigo 35.º, 1.

[4] Versão inicial do artigo 35.º, 2.

[5] Versão (atual) Alterada pelo Artigo 18.º da Lei Constitucional n.º 1/97 – Diário da República n.º 218/1997, Série I-A de 1997-09-20, em vigor a partir de 1997-10-05 do Artigo 35.º, 1.

para tratamento de dados sensíveis, a não ser que haja o consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis[6] e proíbe o acesso a dados pessoais de terceiros, com as devidas exceções legais[7].

À nível europeu, em 23 de setembro de 1980 foram adotadas as Diretrizes da OCDE (Organização para a Cooperação e Desenvolvimento Econômico) sobre a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais, que representam até hoje o consenso internacional sobre a orientação geral relativa à coleta e ao gerenciamento de informações pessoais estabelecendo princípios fundamentais e assistindo governos, empresas e representantes de consumidores em seus esforços para proteger a privacidade e os dados pessoais[8].

À época, as guidelines da OCDE o denominaram de *openness principle*, princípio da abertura, segundo o qual indicava a necessidade de haver uma política geral de abertura sobre as práticas e políticas com relação a dados pessoais. Orientavam que deveriam haver meios que indicassem a existência e a natureza dos dados pessoais, as principais finalidades de seu uso, bem como a identidade e a residência habitual do controlador de dados. [9]

Após, a Convenção 108 do Conselho Europeu de 1981 que teve lugar em Strasbourg foi o principal marco de uma abordagem da matéria de proteção de dados pessoais através da chave dos direitos fundamentais[10], sendo, assim, o primeiro tratado internacional sobre

---

[6] Consoante versão atual do Artigo 35.º, 3.

[7] Consoante versão atual do Artigo 35.º, 4.

[8] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD Publishing, Paris, 2002 Disponível em: https://doi.org/10.1787/9789264196391-en. Acesso em: 03 mar. 2025.

[9] Openness Principle.:

[12.] There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

[10] DONEDA, Danilo. O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coord.). Direito

proteção de dados pessoais. Ele introduziu a ideia de que o tratamento de dados deve ser realizado de forma leal e lícita, um conceito que prefigura o princípio da transparência.

Como se vê o princípio já era dotado de importante valor no tratamento de dados pessoais:

> **Artigo 5 – Legitimidade do tratamento de dados e qualidade dos dados**
> (...)
> 4. Os dados pessoais sujeitos a tratamento deverão ser:
> a. tratados de forma justa e transparente;
>
> **Artigo 8 – Transparência do tratamento**
> 1. Cada Parte deverá prever que o responsável pelo tratamento informa os titulares dos dados sobre:
> (…)
> b. o fundamento jurídico e as finalidades do tratamento previsto;
> (…)
>
> **Artigo 9 – Direitos do titular dos dados**
> 1. Todas as pessoas terão o direito de:
> (...) b. obter, mediante pedido, a intervalos razoáveis e sem demora ou despesas excessivas, a confirmação do tratamento dos dados pessoais que lhe digam respeito, a comunicação, sob forma inteligível, dos dados tratados, toda a informação disponível sobre a sua origem e o período de conservação, bem como qualquer outra informação que o responsável pelo tratamento seja obrigado a fornecer a fim de assegurar a transparência do tratamento nos termos do artigo 8.º, n.º 1;

digital: direito privado e internet. 3. ed. Indaiatuba: Editora Foco, 2020. p.27.

Após a Convenção 108 do Conselho da Europa de 1981, um marco relevante foi a Diretiva 95/46/CE de 24 de Outubro de 1995, aprovada pela União Europeia em 1995. Essa norma consolidou a proteção de dados pessoais, exigindo que os Estados-Membros harmonizassem suas legislações nacionais com as diretrizes estabelecidas. A diretiva abordou aspectos como privacidade, transparência e direitos dos titulares, promovendo um ambiente legal uniforme para a gestão e proteção de informações pessoais em toda a Europa.

Segundo António Barreto Menezes Cordeiro, o princípio da transparência seria uma novidade no RGPD, por considerar que durante a vigência da Diretiva 95/46/CE era abrangido pelo princípio da lealdade[11][12]. O princípio da lealdade estava previsto na alínea a) do n.º 1 do artigo 6.º da Diretiva 95/46/CE:

> **Artigo 6.º**
> 1. Os Estados-membros devem estabelecer que os dados pessoais serão:
> a) Objecto de um tratamento leal e lícito;

Porém, nos Considerandos desta Diretiva já havia a indicação do o dever de transparência do tratamento de dados pelas autoridades de controlo dos Estados-Membros[13]. Além disso, pode-se dizer que o princípio da transparência no tratamento de dados na Diretiva 95/46/CE estava previsto nos arts. 10 e 11, os quais exigiam que o responsável pelo tratamento fornecesse informações claras e acessíveis aos titulares

---

[11] O princípio da lealdade estava previsto no Artigo 6.º, 1, a da Diretiva 95/46/CE
1. Os Estados-membros devem estabelecer que os dados pessoais serão:
a) Objecto de um tratamento leal e lícito;

[12] CORDEIRO, A. Barreto Menezes. Direito da proteção de dados: à luz do RGP e da Lei n.º 58/2019. Coimbra: Almedina, 2022. p.155

[13] (62) Considerando que a criação nos Estados-membros de autoridades de controlo que exerçam as suas funções com total independência constitui um elemento essencial da protecção das pessoas no que respeita ao tratamento de dados pessoais;
(63) (...) que essas autoridades devem ajudar a garantir a transparência do tratamento de dados efectuado no Estado-membro sob cuja jurisdição se encontram;

sobre o processamento de seus dados com o objetivo de garantir que os titulares tivessem plena compreensão de como seus dados seriam utilizados, promovendo confiança e controle.

No RGPD, a transparência é mencionada por diversas vezes ao longo do texto como princípio fundamental do tratamento de dados pessoais, como se vê nas alíneas a) e d) do n.º 1 do artigo 5.º[14] e no artigo12.º[15], além de contar com uma seção inteiramente dedicada para a transparência e o cumprimento dos direitos dos titulares de dados[16][17]. Ainda, conta com uma seção inteiramente dedicada para a transparência e o cumprimento dos direitos dos titulares de dados.

Assim, verifica-se que a transparência no tratamento de dados pessoais consiste em assegurar que os indivíduos sejam informados de maneira clara e acessível sobre a forma como seus dados são coletados, utilizados, armazenados e compartilhados. Esse princípio requer que as informações sejam apresentadas de forma compreensível, permitindo que qualquer pessoa, independentemente de seu nível de conhecimento técnico, possa entender os processos que envolvem seus dados.

---

[14] Artigo 5.º Princípios relativos ao tratamento de dados pessoais

1. Os dados pessoais são:

a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados («licitude, lealdade e transparência»);

(…) d) Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora («exatidão»);

[15] O artigo 12 estabelece as regras gerais que se aplicam a: fornecimento de informações aos titulares de dados (de acordo com os arts. 13 a 14); comunicações com os titulares de dados sobre o exercício de seus direitos (de acordo com os arts. 15 a 22); e comunicações relacionadas a violações de dados (artigo 34).

[16] CAPÍTULO III, Direitos do titular dos dados, Secção 1 Transparência e regras para o exercício dos direitos dos titulares dos dados.

[17] Porém, não há qualquer previsão expressa e detalhada sobre o que, de fato, seja a transparência. No RGPD esta acaba por ser uma norma-princípio, orientando a interpretaçao de outras normas e sua compreensãoé constuída a partir do contexto do RGPD, seus considerandos, da jurisprudência e das orientações do Comitê Europeu para Proteção des Dados. Portanto, a definição é implícita.

No Brasil, a regulação sobre o tema tardou mais a chegar, pelo que a Lei Geral de Proteção de Dados (LGPD)[18] é datada de agosto de 2018 e entrou totalmente em vigor dois anos depois[19]. Porém, ante os desafios da era digital, fez-se necessária para garantir que as pessoas tenham clareza sobre como seus dados são coletados, processados, protegidos e seus direitos.

A LGPD brasileira é uma lei principiológica e prevê o princípio da transparência como um dos princípios que devem reger as atividades de tratamento de dados pessoais, juntamente da boa-fé[20].

Até a entrada em vigor do LGPD a transparência no tratamento de dados pessoais era protegida de forma fragmentada e indireta, sob princípios constitucionais, normas consumeristas e, a partir de 2014, com o Marco Civil da Internet.

Os direitos à inviolabilidade da intimidade e da vida privada e do sigilos das comunicações, previstos no artigo 5.º, incisos X e XII[21] eram interpretados como uma base principiológica para a proteção de dados pessoais e para a exigência de transparência no seu tratamento.

No Código de Defesa do Consumidor[22], datado de 1990, já havia o direito do consumidor acessar as informações existentes em cadastros, fichas, registros e dados pessoais e de consumo sobre ele, bem como suas fontes.[23]

---

[18] Lei n.º 13.709, de 14 de AGOSTO de 2018.

[19] Consoante previsão do artigo 65, II da Lei.

[20] artigo 6.º, caput e VI da LGPD.

[21] artigo 5.º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

(…) X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

(…) XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

[22] Lei n.º 8.078, de 11 de setembro de 1990 – Dispõe sobre a proteção do consumidor e dá outras providências.

[23] artigo 43 do CDC.

Ademais, o Marco Civil da Internet[24] também trata da proteção dos dados pessoais, prevendo o consentimento na coleta dos dados e o agir de maneira transparente. Foi um dos instrumentos mais relevantes no contexto digital brasileiro pré-LGPD, demonstrando a necessidade da transparência e do consentimento informado nas relações firmadas no contexto da internet.

Assim, vê-que a transparência tem como objetivo fortalecer a confiança dos titulares ao promover práticas que respeitem seus direitos e assegurem maior controle sobre suas informações pessoais, sendo um aspecto central nas regulamentações modernas de proteção de dados, como o RGPD na Europa e a LGPD no Brasil.

b. Noção de transparência

Danilo Doneda sintetiza o princípio da publicidade ou da transparência, como aquele "pelo qual a existência de um banco de dados pessoais deve ser de conhecimento público, seja através da exigência de autorização prévia para funcionar, da notificação a uma autoridade sobre sua existência ou do envio de relatórios periódicos".[25]

A transparência no tratamento dos dados pessoais não se limita à mera transferência de informações de um agente a outro: é complexa pois pode se referir à capacidade de explicação do tratamento dos dados, à capacidade de interpretação, acessibilidade, abertura e visibilidade deste[26].

Segundo Filipe Magalhães, o direito à transparência tendo como principais destinatários os titulares de dados pessoais nada mais é do

---

[24] Lei n.º 12.965, de 23 de abril de 2014 – Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

[25] DONEDA, Danilo. O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS. p.26.

[26] FÁCIO, Rafaella Nátaly. "A transparência e o direito de acesso no tratamento de dados pessoais: considerações sobre intersecções entre Lei Geral de Proteção de Dados e Lei de Acesso à Informação no Brasil." *Rev. Eurolatin. de Derecho Adm.*, Santa Fe, v. 10, n. 2, e247, jul./dic. 2023.p.8

que a consagração da necessidade de utilização de uma linguagem e procedimentos transparentes[27].

O princípio da transparência está presente em todas as etapas do tratamento de dados, abrangendo desde os primeiros contatos entre o responsável pelo tratamento e os potenciais titulares de dados (fase de formação), passando pela coleta e pelas demais operações de tratamento (fase de execução), mantendo-se aplicável mesmo após o encerramento da relação.[28]

Apesar de não haver uma definição expressa de transparência no RGPD, o considerando 39 do é informativo quanto ao seu significado e ao efeito do princípio da transparência no contexto do processamento de dados[29]:

> (39) O tratamento de dados pessoais deverá ser efetuado de forma lícita e equitativa. Deverá ser transparente para as pessoas singulares que os dados pessoais que lhes dizem respeito são recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento e a medida em que os dados pessoais são ou virão a ser tratados. **O princípio da transparência exige que as informações ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples. Esse princípio diz respeito, em particular, às informações fornecidas aos titulares dos dados sobre a identidade do responsável pelo tratamento dos mesmos e os fins a que o tratamento se destina, bem como às informações que se destinam a assegurar que seja efetuado com equidade e transparência para com as pessoas singulares em causa, bem como a salvaguardar o seu direito a obter a**

[27] MAGALHÃES, Filipe. *Manual RGPD*. Ordem dos Contabilistas Certificados (OCC), 2018. p.13.

[28] CORDEIRO, A. Barreto Menezes. Direito da proteção de dados, p.154

[29] Article 29 Data Protection Working Party. **Guidelines on transparency under Regulation 2016/679**. Adopted on 29 November 2017. Revised and adopted on 11 April 2018. Disponível em: https://ec.europa.eu/newsroom/article29/items/622227. Acesso em: 06 fev 2025.

> **confirmação e a comunicação dos dados pessoais que lhes dizem respeito que estão a ser tratados**. As pessoas singulares a quem os dados dizem respeito deverão ser alertadas para os riscos, regras, garantias e direitos associados ao tratamento dos dados pessoais e para os meios de que dispõem para exercer os seus direitos relativamente a esse tratamento. (grifo nosso)

A LGPD brasileira prevê explicitamente a noção do princípio da 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."[30].

Trata-se de um princípio que se converte em uma regra jurídica, como se vê do § 1.º do artigo 9.º, que considera nulo o consentimento que não tenha cmprido com informar de forma transparente, clara e inequívoca o titular dos dados[31].

2. O Tratamento de Dados Pessoais na Internet

a. Caracterização de dados pessoais e sensíveis na era digital

Dado pessoal, enquanto, "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»)" consoante artigo 4.º, n.º 1 do RGPD, e, do mesmo modo, "informação relacionada a pessoa natural identificada ou identificável" no artigo 5.º, n.º 1 da LGPD, é facilmente vinculada à informações que aparecem em sistemas eletrônicos, mas também nas vias físicas.

---

[30] artigo 6.º, VI

[31] artigo 9.º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: (…) § 1.º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca. (grifo da autora)

No ambiente digital, a coleta de dados pessoais tornou-se ampla e constante, frequentemente ocorrendo sem que os indivíduos tenham plena ciência ou forneçam consentimento expresso. Serviços online, redes sociais, aplicativos e plataformas digitais acessam grandes volumes de informações pessoais por meio de práticas como monitoramento contínuo, análise de metadados e aplicação de algoritmos que antecipam comportamentos, muitas vezes de maneira pouco evidente para os usuários.

Portanto, cabe nominar exemplos de dados pessoais específicos do uso da internet. Primeiramente, informações de navegação online são consideradas dados pessoais, como endereços IP (protocolo internet), cookies (testemunhos de conexão), comportamento de navegação e histórico de buscas. Ademais, dados de localização do usuário (titular dos dados), como informações sobre onde o usuário se encontra em tempo real por meio de dispositivos móveis e aplicativos.

Os metadados são informações como hora e data de envio de e-mails, mensagens ou interações em plataformas digitais. Ao associá-los com outros dados, permitem identificar o seu titular, por exemplo.[32] No âmbito das redes sociais, perfil do usuário, seus posts, as fotos postadas, interações, etc, também são considerados dados pessoais.

Em tratando-se de dados sensíveis de um subconjunto dos dados pessoais que podem revelar aspectos íntimos da vida do indivíduo, exigem um nível mais alto de proteção, como se vê do Considerando 51[33] e do artigo 9.º do RGPD e do artigo 11 da LGPD.

---

[32] "A palavra metadados significa algo como "*além dos dados*". Dito de outra forma, os metadados são dados sobre outros dados, ou seja, permitem auxiliar na identificação, descrição e localização de informação." Ver: https://www.cgd.pt/Site/Saldo-Positivo/formacao-e-tecnologia/Pages/metadados-o-que-sao.aspx#:~:text=para%20que%20serve–,O%20que%20s%C3%A3o%20os%20metadados%3F,descri%C3%A7%C3%A3o%20e%20localiza%C3%A7%C3%A3o%20de%20informa%C3%A7%C3%A3o. Acesso em 11 ago 2025.

[33] "Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais.(…)"

Assim, em meio digital, os dados sensíveis são aqueles de origem racial ou étnica obtidos através de plataformas que coletam dados sobre a aparência, comportamento ou preferências culturais, incluindo redes sociais. Igualmente, opiniões políticas e crenças religiosas compartilhadas em redes sociais ou coletadas por serviços de publicidade online. Ainda, dados sobre a saúde do usuário como históricos médicos, tratamentos, diagnósticos e informações sobre condições de saúde compartilhadas em aplicativos ou dispositivos de monitoramento de saúde, como os relógios inteligentes.[34] Informações baseadas em comportamentos online sobre a vida sexual e/ou orientação sexual do usuário[3536], como as interações realizadas em plataformas de namoro ou consumo de conteúdo são consideradas dados pessoais sensíveis.

Há de se falar também nas informações extraídas de tecnologias de reconhecimento facial, impressões digitais, muitas vezes coletadas em aplicativos de segurança ou plataformas que utilizam autenticação biométrica, e informações sobre DNA obtidas em sites de testes genéticos[37]: trata-se de dados biométricos e genéticos, portanto, são dados pessoais sensíveis.

Os dados sensíveis se tornaram ainda mais acessíveis e suscetíveis a abusos na era digital, principalmente devido à utilização massiva de tecnologias de coleta e inteligência artificial, que podem processar grandes volumes de dados e inferir informações sensíveis a partir de comportamentos ou padrões de consumo. Por isso, a transparência

---

[34] Consoante definição do artigo 5.º, II da LGPD e artigo 9.º, 1 do RGPD.

[35] Apesar do rol de dados sensíveis previsto na LGPD não incluir expressamente "orientação sexual" e "identifdade de gênero", indica que a informação acerca da vida sexual de um sujeito é um dado sensível.

[36] Ver: FICO, Bernardo de Souza Dantas; NÓBREGA, Henrique Meng. "The Brazilian Data Protection Law for LGBTQIA+ People: Gender identity and sexual orientation as sensitive personal data" Revista Direito e Práxis, v. 13, n. 2, p. 1262–1288, 2022.

Disponível em: https://www.e-publicacoes.uerj.br/revistaceaju/article/view/66817. Acesso em: 19 abr. 2025.

[37] "Dados genéticos são o que há de mais pessoal e não podem ser alterados. Caso haja uma violação de dados, por exemplo, o indivíduo fica exposto definitivamente. Não é como a senha do Facebook, que basta alterar e atualizar em todos os dispositivos para garantir sua segurança novamente." BERTOLLI, Emilia.Os riscos dos testes genéticos. *Varonis*, 2023. Disponível em: https://www.varonis.com/pt-br/blog/os-riscos-dos-testes-geneticos. Acesso em: 20 jan. 2025.

acerca do processamento dos dados pessoais dos usuários é de extrema importância no quotidiano dos internautas.

b. Os desafios da coleta e armazenamento de dados na internet

A proteção de dados pessoais e sensíveis na era digital envolve desafios complexos, dentre eles, a coleta em massa, armazenamento e compartilhamento de dados, decisões automatizadas e discriminação algorítmica.

No que diz respeito à coleta em massa de dados pessoais na internet, há de sew falar na consequente invasão da privacidade do titular destes. Essa coleta é muitas vezes realizada sem o conhecimento do titular, utilizando tecnologias como rastreamento de localização e monitoramento de comportamento online, o que gera insegurança jurídica.

Ainda, é um fato inegável que a natureza transfronteiriça da internet permite a armazenagem de dados em servidores do mundo todo, o que acaba por dificultar a proteção. Daí a importância da transparência quando houver a intenção de tratamento dos dados, de forma a obter um consentimento lícito.

Dados aparentemente inocentes como um número de telefone associado ao artigo comprado em determinada loja virtual permitem o estabelecimento de um perfil de consumo sobre um sujeito, principalmente quando associado a informações vindas de outras bancos de dados.[38]

Ademais, identificadores fornecidos pelos aparelhos eletrônicos, aplicações, ferramentas e protocolos podem deixar vestígios que, em especial quando combinados com identificadores únicos e outras informações recebidas pelos algoritmos, podem ser utilizados para a definição de perfis e a identificação das pessoas singulares.[39]

---

[38] Sobre a possibilidade de identificar um sujeito com base no comportamento online e poucos dados pessoais, ver: RUIZ, Evandro Eduardo Seron. Anonimização, pseudonimização e desanonimização de dados pessoais. Comentários à Lei Geral de Proteção de Dados – Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019. São Paulo: Almedina Brasil, 2020. Pp.104-105

[39] Considerando 30 do RGPD

O uso de inteligência artificial é cada vez mais usual nas práticas de publicidade e no tratamento de dados pessoais, o que, com base em dados estatísticos e as "regras" que alimentaram o algoritmo existente, podem levar à uma discriminação indireta, prejudicando determinados grupos de pessoas com base em dados sensíveis, como etnia ou orientação sexual.

c. A transparência como dever: obrigações legais nos regimes de proteção dos dados pessoais

Em aspectos práticos há de se levar em conta o considerando 58 do Regulamento, o qual clarifica a forma como deve se dar a informação ao titular dos dados: "concisa, de fácil acesso e compreensão, bem como formulada numa linguagem clara e simples, e que se recorra, adicionalmente, à visualização sempre que for adequado", podendo ser fornecidas por via eletrónica.

Consoante os direitos de informação e acesso presentes nos arts. 13.º a 15.º do RGPD, os titulares dos dados têm o direito de ser informados pelos responsáveis pelo tratamento de dados sobre a existência de decisões automaticamente e de receber informações sobre a lógica envolvida e as consequências previstas deste tratamento automatizado[40], bem como de receber detalhes sobre os seus dados pessoais que estão a ser utilizados para *automated decision-making* (ADM) [41].

Segundo Barbosa, estes direitos de informação e acesso podem ser entendidos como um direito a uma explicação genérica *ex ante* sobre a funcionalidade do sistema e as suas consequências para a pessoa em causa, embora o direito a uma explicação *ex post* não esteja incluído na disposição[42].

---

[40] Consoante arts. 13.º, n.º 2, alínea f), e 14.º, n.º 2, alínea g).

[41] artigo 15.º, n.º 1, alínea h).

[42] BARBOSA, Sandra. A importância da transparência e explicabilidade no uso de decisões automatizadas pelo artigo 22.º do RGPD. Cadernos de Proteção de Dados da União Europeia, Lisboa: CEDIS, Faculdade de Direito da Universidade Nova de Lisboa, 2022. Disponível em: https://protecaodedadosue.cedis.fd.unl.pt/wp-content/uploads/2022/10/3.-Sandra-Barbosa.pdf.

Como consequência da transparência, tem-se os direitos de acesso, retificação, apagamento e portabilidade, os quais encontram-se previstos nos artigos 15 a 22 com a forma de exercê-los. Além disso, há a salvaguarda do direito de "obter intervenção humana" mencionado no artigo 22.º, a que se convencionou chamar "direito à explicação" com base na expressão "obter uma explicação sobre a decisão tomada" utilizada no considerando 71 do Regulamento.

Ao estabelecer a obrigação de o controlador informar os titulares sobre violações de dados pessoais que representem alto risco aos seus direitos e liberdades, o artigo 34.º do RGPD acaba por concretizar, de algum modo, o princípio da transparência.[43]

Ainda, é possível afirmar que a designação do Encarregado de Proteção de Dados (DPO), ao garantir que exista uma figura responsável por supervisionar o cumprimento da legislação e facilitar a comunicação entre o controlador, os titulares de dados e as autoridades de supervisão, seja uma materialização do princípio da transparência. Isso porque a presença do DPO promove clareza e acessibilidade para os titulares, que podem vir a buscar informações ou exercer seus direitos, reforçando a transparência nos processos de tratamento de dados pessoais.

Na LGPD brasileira, o princípio da transparência (artigo 6.º, VI)[44], juntamente do princípio do livre acesso (artigo 6.º, IV)[45], dá origem ao direito de acesso aos dados pessoais[46], este, que por sua vez, é consolidado pelos artigos 18 e 19[47]:

Acesso em: 17 jan. 2025. p.70

[43] Essa comunicação deve ser clara, compreensível e fornecer detalhes sobre a natureza da violação, os possíveis impactos e as medidas adotadas. Assim, promove-se a transparência ao garantir que os titulares sejam informados de forma adequada e possam tomar medidas para proteger seus interesses.

[44] (...) IV – 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;

[45] (...) IV – 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;

[46] artigo 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: I – confirmação da existência de tratamento; II – acesso aos dados;(...)

[47] SCHLOTTFELDT, Shana. REVISÃO DE DECISÃO TOMADA COM BASE EM

> artigo 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> I – confirmação da existência de tratamento;
> II – acesso aos dados;
> (…)
> VII – informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> VIII – informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> (…)
>
> artigo 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:
> I – em formato simplificado, imediatamente; ou
> II – por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular. (…)

Juntos, estes dispositivos permitem ao titular tomar conhecimento dos dados utilizados para as decisões automáticas, além da forma e da duração do tratamento.

Ademais, derivado do princípio da transparência, há de se falar no princípio da qualidade dos dados previsto no artigo 6.º V[48], que permite

---

TRATAMENTO AUTOMATIZADO: PREOCUPAÇÕES E CONSIDERAÇÕES SOBRE A EFETIVAÇÃO DA TRANSPARÊNCIA PARA COBRIR A DISCRIMINAÇÃO ALGORÍTIMICA E O PROFILING. In: MENDES, Laura Schertel Ferreira (Org.) et al. Anuário do Observatório da LGPD da Universidade de Brasília: análise comparada entre elementos da LGPD e do GDPR. Brasília: Universidade de Brasília, Faculdade de Direito, 2024. 2 v. pp. 117-136

[48] Artigo 6.º (...) V – 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;

que o titular demande a atualização e a correção de dados incompletos, inexatos ou desatualizados (artigo 18, III[49]).[50] Igualmente, se materializa através dos direitos à oposição e à exclusão (artigo18, VI)[51] e o princípio da não-discriminação (artigo 6.º, IX)[52], acionado caso o titular suponha estar sofrendo discriminação em razão do tratamento dos seus dados.

É imperioso que seja dessa forma ante a velocidade do avanço da tecnologia e do caráter transfronteiriço da internet, pelo que sem a devida transparência se torna praticamente impossível o controle pelo titular do fluxo de seus dados, bem como quaisquer fiscalizações pelos órgãos de controle.[53]

Por último, mas não menos importante, há de se falar na possibilidade de revisão de decisões automatizadas, previsto no artigo 20, *caput*, o que sugere acesso sempre em momento posterior à coleta de dados e desenvolvimento do algoritmo que os processa[54].

---

[49] artigo 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: (…) III – correção de dados incompletos, inexatos ou desatualizados;

[50] SCHLOTTFELDT, Shana. REVISÃO DE DECISÃO TOMADA COM BASE EM TRATAMENTO AUTOMATIZADO: PREOCUPAÇÕES E CONSIDERAÇÕES SOBRE A EFETIVAÇÃO DA TRANSPARÊNCIA PARA COBRIR A DISCRIMINAÇÃO ALGORÍTIMICA E O PROFILING. In: MENDES, Laura Schertel Ferreira (Org.) et al. Anuário do Observatório da LGPD da Universidade de Brasília: análise comparada entre elementos da LGPD e do GDPR. Brasília: Universidade de Brasília, Faculdade de Direito, 2024. 2 v. pp. 117-136

[51] artigo 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: (...) VI – eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no artigo 16 desta Lei;

[52] IX – não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

[53] FLUMIGNAN, Silvano José Gomes; FLUMIGNAN, Wévertton Gabriel Gomes. Princípios que Regem o Tratamento de Dados no Brasil. In: LIMA, Cíntia Rosa Pereira de (Coord.) Comentários à Lei Geral de Proteção de Dados: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019. São Paulo: Almedina, 2020. p.132.

[54] FERNANDES, Micaela Barros Barcelos; OLIVEIRA, Camila Helena Melchior Baptista de. "O artigo 20 da LGPD e os desafios interpretativos ao direito à revisão das decisões dos agentes de tratamento pelos titulares de dados." Revista de Direito e as Novas Tecnologias. V.8/2020, jul.-set./2020

3. Algoritmos, Inteligência Artificial e os Desafios de Transparência

a. O processamento de dados pessoais pelos algoritmos

Os dados pessoais ganharam importância mercadológica enorme conforme o avanço tecnológico passou a permitir a vinculação destes a pessoas reais, tornando-se uma extensão de suas personalidades no meio digital. A possibilidade de processar grandes bases de dados por algoritmos permitiu a criação de ferramentas cada vez mais precisas e capazes de prever tendências e comportamentos humanos.[55] Segundo o ChatGPT[56], um algoritmo é uma sequência finita de instruções bem definidas e ordenadas que, quando executadas, visam resolver um problema específico ou realizar uma tarefa determinada.[57]

É um fato inegável que os algoritmos são alimentados por dados[58-59]. Com base nestes, algoritmos que usam da inteligência artificial podem vir a negar crédito a pessoas, demitir ou contratar pessoas com base em seus dados ou padrões estatísticos dos dados que possui, dentre outras situações que podem ocorrer. Assim que os algoritmos

---

[55] WANDERER, Bertrand. Economia movida a dados e o papel das plataformas digitais. Journal of Law and Regulation, v. 9, n. 2, p. 22–43, 2023. p.26.

[56] "Embora o ChatGPT possa ser tecnicamente descrito como um algoritmo de IA, sua complexidade o aproxima mais de um modelo estatístico baseado em aprendizado de máquina, diferindo dos algoritmos tradicionais em sua forma de funcionamento, transparência e interpretabilidade." OPENAI. Resposta gerada pelo modelo ChatGPT. Disponível em: https://chat.openai.com/. Acesso em: 06 fev. 2025.

[57] OPENAI. Resposta gerada pelo modelo ChatGPT. Disponível em: https://chat.openai.com/. Acesso em: 21 jan. 2025.

[58] RIBEIRO, Elieser. "A potência dos dados para a inteligência artificial." Medium, 17 ago. 2020. Disponível em: https://medium.com/@elieser_ribeiro/a-pot%C3%AAncia-dos-dados-para-a-intelig%C3%AAncia-artificial-703f1c05750f. Acesso em: 21 jan. 2025.

[59] "Sim, é correto afirmar que um algoritmo é alimentado por dados. Um algoritmo utiliza entradas (dados) para executar sua sequência de instruções e produzir saídas (resultados). Esses dados podem ser estáticos (pré-definidos) ou dinâmicos (fornecidos em tempo real), e sua qualidade e relevância são cruciais para o desempenho e a precisão do algoritmo, especialmente em sistemas baseados em aprendizado de máquina." OPENAI. Resposta gerada pelo modelo ChatGPT para a seguinte pergunta: "é correto afirmar que o algoritmo é alimentado por dados?". Disponível em: https://chat.openai.com/. Acesso em: 21 jan. 2025.

estão presentes no dia a dia da população sem que muitas vezes saiba: vive-se numa verdadeira vigilância algorítmica.[60]

Segundo o Regulamento de IA europeu, entende-se por Sistema de IA:

> (...) um sistema baseado em máquinas concebido para funcionar com níveis de autonomia variáveis, e que pode apresentar capacidade de adaptação após a implantação e que, para objetivos explícitos ou implícitos, e com base nos dados de entrada que recebe, infere a forma de gerar resultados, tais como previsões, conteúdos, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais.[61]

Para além dos algoritmos tradicionais, há de se falar na técnica de aprendizagem de máquina (*machine learning*)[62], impulsionada pela explosão do volume de dados digitais. Nessa, os sistemas são expostos a um grande número de exemplos (dados) e devem extrair deles padrões recorrentes.[63]

---

[60] "Dataveillance is the systematic creation and/or use of personal data for the investigation or monitoring of the actions or communications of one or more persons." CLARKE, Roger; GREENLEAF, Graham. Dataveillance Regulation: A Research Framework. UNSW Law Research Series, 7 nov. 2017. P.3.

[61] Artigo 3.º (1) do Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho de 13 de junho de 2024 que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.o 300/2008, (UE) n.o 167/2013, (UE) n.o 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial).

[62] O termo "aprendizado de máquina" (machine learning, em inglês) faz referência a um método algorítmico que permite a um sistema chegar a conclusões mediante tentativas e erros, até alcançar o resultado almejado. O sistema aprende com seus erros em uma espécie de inteligência artificial. Entre as modalidades de aprendizado de máquina, existe o "aprendizado profundo" (deep learning, em inglês), que utiliza sistemas paralelos para aprender e, muitas vezes, seu resultado final pode ser diferente do antevisto por quem desenvolveu o algoritmo. Ver: BURRELL, Jenna. "How the machine 'thinks': Understanding opacity in machine learning algorithms. Big Data & Society, v. 3, n. 1. SAGE Publications, 2016.

[63] DEVILLÉ, Rembrandt; SERGEYSSELS, Nico; MIDDAG, Catherine. Basic Concepts of AI for Legal Scholars. In: BRUYNE, Jan De; VANLEENHOVE, Cedric (ed.). Artificial Intelligence and the Law. Antuérpia: Intersentia, 2021. p. 1-22, p. 5.

A depender da forma como os dados são apresentados ao sistema, a aprendizagem de máquina pode seguir diferentes metodologias. Na aprendizagem supervisionada, o algoritmo é treinado com exemplos cujas respostas corretas já são conhecidas, permitindo-lhe ajustar seus parâmetros com base nesse feedback. Na aprendizagem não supervisionada, o sistema apenas recebe dados brutos e deve, por si só, identificar agrupamentos, relações ou estruturas internas.[64]

Em razão desta capacidade dos algoritmos de gerar um padrão comportamental dos sujeitos através de uma correlação dos dados que possui, surge a preocupação com os dados pessoais que os alimentam.[65]

Inclusive, o artigo 4.º, n.º 4 do RGPD aborda o *profiling* com ênfase em uso para previsão comportamental. E, para que seja caracterizado como criação de perfil, há de haver algum processamento automatizado, pelo que qualquer participação humana no processo não descaracteriza o fenômeno[66].

Há de se falar, também, que em sistemas mais complexos, as sequências pré-definidas podem ser alteradas de acordo com os dados que os alimentam e também pelas conclusões intermediárias. Essa natureza adaptativa tem se tornado mais comum nos sistemas de inteligência artificial e aprendizado de máquina capazes de influenciar as conclusões intermediárias – de modo que não seja mais possível prever os resultados finais ou entender sua lógica subjacente.[67]

---

[64] Ibidem, p.6.

[65] ABRANTES, Paula Cotrim de. "Desafios e dilemas da proteção de dados pessoais na era da cultura algorítmica." In: SciELO Preprints. DOI 10.1590/SciELOPreprints.7141. p. 1-27, 2023. p.11.

[66] Article 29 Working Party. 2018. Guidelines on Autoimated «individual decision-making and Profiling for the purposes of Regulation 2016/679. WP251revb.01

[67] "Algoritmos baseados em metodologias de aprendizado de máquina e aprendizado profundo podem chegar a várias conclusões intermediárias antes de atingir o seu resultado final. Estas servem para ensinar o algoritmo a atingir o resultado correto, a partir de tentativa e erro, ou até mesmo alterar o algoritmo para atingir outros resultados, alguns deles não antevistos por seus desenvolvedores." MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? Rio de Janeiro: Instituto Igarapé, 2018. 27 p. (Artigo Estratégico, 39). p.2.

Segundo Goodman e Flaxman, algoritmos de aprendizado de máquina supervisionado para regressão ou classificação são baseados na descoberta de associações e/ou correlações confiáveis para auxiliar na previsão precisa fora da amostra, sem a preocupação acerca do raciocínio causal ou de explicação para além do sentido estatístico, através do qual é possível medir a quantidade de variância explicada por um preditor.[68] Daí surge a preocupação com a transparência destes processos.

Essa complexidade pode ser entendida como opacidade, vez que impede que as pessoas entendam e verifiquem se seus dados pessoais são tratados de forma legítima, adequada e proporcional. Daí surge uma preocupação: a falta de transparência sobre o funcionamento dos algoritmos indica a tendência de que esses mecanismos venham a segregar determinadas informações, privilegiem outras, reproduzindo padrões de preconceito e discriminação, reforçando, assim, o aprofundamento das desigualdades da sociedade[69-70].

Essa opacidade pode se apresentar em diferentes formas: a opacidade intencional por parte de corporações ou instituições que mantém seus processos de tomada de decisão longe do escrutínio público;[71] a opacidade enquanto falta de conhecimento técnico[72], a qual decorre do reconhecimento de que compreender a operação é uma habilidade especializada restrita a minoria da população; e a opacidade de quando há desalinhamento entre as complexas operações matemáticas por certos

---

[68] GOODMAN, Bryce; FLAXMAN, Seth. European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation". AI Magazine, v. 38, n. 3, p. 50-57, 2017. p. 6.

[69] Vê-se o uso desse tipo de inteligência artificial em atividades como processos seletivos para empregos, aplicação de tarifas de planos de saúde, obtenção de crédito, dentre outros.

[70] Nesse sentido, Cathy O'NEIL já considerou os algoritmos como armas de destruição matemática: O'NEIL, Cathy. Weapons of math destruction: how big data increases inequality and threatens democracy. New York: Crown Publishing Group, 2016.

[71] Segundo Diego Machado, pode se dar através do uso de técnicas computacionais para controlar a burla do sistema e da tutela jurídica do segredo comercial ou industrial para ofuscar o real funcionamento do algoritmo. MACHADO, Diego. Algoritmos e Proteção de Dados Pessoais. São Paulo: Almedina, 2023. E-book. p.178.

[72] Chamado por Jenna Burrell, de "Opacity as technical illiteracy", em tradução livre "opacidade como analfabetismo técnico". Burrell, Jenna. How the machine "thinks": Understanding opacity in machine learning algorithms. Big Data & Society, 2016 3(1), p.4.

algoritmos de aprendizado de máquina e a interpretação feita pelo ser humano.[73]

Colocando o direito à proteção de dados pessoais em perspectiva, a existência de opacidade e invisibilidade no processo de formação e de aplicação do perfilamento automatizado confronta a própria configuração deste direito fundamental como instrumento de transparência. A opacidade pontuada pode criar verdadeiros embaraços ao uso de mecanismos de controle e responsabilização do poder exercido por agentes de tratamento, públicos ou privados. Isso somado da invisibilidade ou dificuldade de compreensão das aplicações tecnológicas, pelo que cresce o perigo de inviabilizar a contestabilidade das operações de tratamento e decisões automatizadas, ferindo a participação dos titulares dos dados no processo de tomada de decisão algorítmica.

Porém, nesse contexto torna-se necessário reconhecer que a intensidade e a natureza dos riscos associados à opacidade algorítmica e o consequente impacto sobre a privacidade podem variar de acordo com a interação realizada entre o titular dos dados (usuário) e a tecnologia, o processamento adotado e o grau de intermediação da inteligência artificial.

No caso do uso individual de um navegador ou de uma aplicação proprietária de IA generativa – como o ChatGPT, Copilot e Gemini, os dados introduzidos pelo utilizador, bem como os de interação, são processados e armazenados em servidores externos, sob regime jurídico e técnico definido pelo fornecedor, com elevada possibilidade de transferência internacional e reutilização para fins de treino.[74] [75]

---

[73] MACHADO, Diego. Algoritmos e Proteção de Dados Pessoais. São Paulo: Almedina, 2023. E-book. p.178.

[74] "The terms say ChatGPT may automatically collect personal information and usage information about a user's use of the services, such as the types of content that they view or engage with, the features they use and the actions they take. The terms say OpenAI may use the data users provide to improve their future models. (...)However, the terms do not disclose whether ChatGPT can display targeted advertisements to users, send third-party marketing communications, or track users based on their interactions with ChatGPT on other apps or services across the internet for advertising purposes." COMMON SENSE. Privacy Evaluation for ChatGPT. 26 jan. 2024. Disponível em: https://privacy.commonsense.org/evaluation/ChatGPT Acesso em 10 ago 2025. Ver também: OpenAI. How your data is used to improve model performance. Disponível em: https://help.openai.com/en/articles/5722486-how-your-data-is-used-to-improve-model-performance Acesso em 11 ago 2025.

[75] Em se tratando de metadados de interação (data e hora da solicitação, endereço IP,

De outro lado, ao utilizar plataformas de redes sociais, o titular de dados, apesar de não necessariamente interagir diretamente com a IA, permanece sujeito à análise comportamental e à segmentação algorítmica não transparente, cujo processamento decorre de observação contínua e agregada, tornando mais difícil a percepção e a contestação do tratamento.

Tal diversidade de contextos impõe que a concretização do princípio da transparência seja sensível à configuração técnica do tratamento, pois o grau de exposição e as salvaguardas necessárias variam substancialmente em função da arquitetura adotada. Considerando os potenciais riscos para os interesses e direitos do titular dos dados, uma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis é vedada pelo artigo 22, n.º 1 do RGPD[76]. A LGPD, ainda que inspirada na norma europeia, não proíbe o tratamento totalmente automatizado de dados. Muito pelo contrário, ela o autoriza no artigo 20, prevendo o direito à revisão como forma de proteção aos titulares.

b. Transparência no uso de algoritmos

Na maioria das vezes, as pessoas não sabem o peso dos seus dados utilizados pelos algoritmos e quais fatores são levados em consideração para a tomada de decisão. Se não houver a devida transparência, a probabilidade de que a programação do algoritmo esteja permeada de vieses e preconceitos dos programadores, intencionais ou não, que

parâmetros técnicos da sessão, tipo de dispositivo e navegador, etc.), estes podem ser processados com a finalidade de prestar o serviço, manter a segurança operacional e, salvo manifestação em contrário do utilizador, contribuir para o treino e melhoria dos modelos de linguagem. Tal enquadra-se no previsto no artigo 4.º, n.º 2, do RGPD e no artigo 5.º, X, da LGPD, abrangendo tratamento de dados desde a coleta até o armazenamento, independentemente de o dado ser textual ou técnico (metadado).

[76] O termo "direito" contido nesta disposição não significa que o artigo 22.º, n.º 1, seja aplicável somente quando ativamente invocado pelo titular dos dados. O artigo 22.º, n.º 1 estabelece uma proibição geral da tomada de decisões com base exclusivamente no tratamento automatizado, a qual aplica-se independentemente de o titular dos dados adotar uma medida relativa ao tratamento dos seus dados pessoais.

podem levar a erros de diagnóstico e a graves discriminações é altíssima. Além disso, é possível que as correlações encontradas no processamento sejam consideradas causalidades de forma equivocada, reforçando discriminações[77].

Segundo Castelluccia e Métayer, transparência não significa necessariamente disponibilidade para o público, mas a disponibilidade para agente de auditoria ou certificação da codificação do processo de tomada de decisões com sua documentação de projeto, parâmetros e o conjunto de dados de aprendizado quando a tomada de decisão algorítmica se baseia no aprendizado de máquina.

Já a explicabilidade seria a disponibilidade de explicações sobre o processo de tomada de decisões, exigindo-se o fornecimento de informações além da própria tomada de decisão algorítmica. Explicações estas que podem ser de diferentes operacionais, causais, globais (sobre todo o algoritmo) ou sobre resultados específicos. Ademais, há de haver diferentes modos de explicação a depender dos destinatários desta (por exemplo, profissionais ou indivíduos), seu nível de especialização e seus objetivos (contestar uma decisão, tomar medidas para obter uma decisão, verificar a conformidade com as obrigações legais etc.).

Quando o algoritmo toma decisões baseadas em regras predefinidas é mais fácil de haver a explicação, providenciando a informação do tratamento de forma compreensível ao usuário, como o princípio da transparência exige. Porém, em se tratando de machine learning, como demonstrado, há uma dificuldade a ser enfrentada.

Em âmbito europeu, no que diz respeito à tomada de decisões automatizada, o princípio da transparência, ao lado da legalidade e da equidade devem reger a utilização e a criação de algoritmos, que por sua vez, tratam e processam dados pessoais, consoante o artigo 5.º, n.º1, alínea a) do RGPD.

---

[77] FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coords.). Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019. p. 39.

Assim, o responsável pelo tratamento de dados tem a transparência enquanto base dos seus deveres, pelo que deve certificar-se de que explique de forma clara e inteligível aos titulares dos dados estes processos, as suas consequências e fornece-lhes ferramentas para agirem contra eles, se assim o pretenderem[78], ou seja, deve informar a pessoa em causa sobre a lógica subjacente aos algoritmos. É possível afirmar que a transparência seja uma das principais formas de compreensibilidade do processo de tomada de decisões pelo algoritmo.

Alinhando-se com os requisitos de informação e acesso presentes nos arts. 13.º a 15.º do RGPD, enquanto forma de materialização da transparência, a informação fornecida tem de abordar quais os dados que foram recolhidos, que estão a ser processados ao abrigo desses meios, e as suas consequências[79]. Ademais, o princípio do tratamento transparente exige que o titular dos dados seja informado da definição de perfis e das consequências que daí advêm[80]. Portanto publicidade direcionada frutos de *profiling* deveriam dar um tratamento transparente de seus dados.

O uso de algoritmos cada vez mais corriqueiro no *online*, especialmente nos sistemas de recomendação e de publicidade direcionada coloca a transparência no tratamento dos dados pessoais nesse contexto no centro do direito digital europeu para além do RGPD. Tanto o Regulamento dos Mercados Digitais (DMA) quanto no Regulamento dos Serviços Digitais (DSA)[81] tratam expressamente deste tema.

O DMA impõe aos gatekeepers a obrigação de divulgar, de forma clara e acessível, os critérios utilizados nos sistemas de recomendação e a lógica utilizada, para que os usuários possam entender por qual razão

---

[78] BARBOSA, Sandra. "A importância da transparência e explicabilidade no uso de decisões automatizadas pelo artigo 22.º do RGPD." p.82

[79] Idem, p.70

[80] Considerando 60 do RGPD.

[81] Ambos os regulamentos Digital Markets Act (DMA) e Digital Services Act (DSA) são frutos do pacote legislativo da União Europeia chamado Pacote dos Serviços Digitais – Digital Services Package. Ver: Digital services package. Disponível em: https://www.consilium.europa.eu/en/policies/digital-services-package/

determinados conteúdos lhes são exibidos[82]. O DSA reforça essa perspectiva ao exigir que as plataformas digitais informem, inclusive nos casos de anúncios personalizados, se houve uso de dados pessoais e com base em quais parâmetros estes lhe foram direcionadas, além de proibir a segmentação com base em dados sensíveis[83].

Conforme anteriormente demonstrado, a LGPD brasileira prevê, no seu artigo 20, aos titulares o direito à revisão das decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses. E como pressuposto ao exercício desse direito, previu que o titular dos dados deverá tenha acesso, sempre que solicitado, a informações claras e adequadas sobre os procedimentos utilizados para se chegar a decisões que interfiram em sua esfera jurídica, resguardando-se os segredos comercial e industrial do controlador (artigo 20 § 1.º, da LGPD).

c. A tensão entre inovação tecnológica e proteção de dados

É fato que os algoritmos funcionam transformando dados de entrada em resultados com base em regras estabelecidas e objetivos previamente definidos, como a identificação de padrões ou correlações. No entanto, compreender plenamente como determinados resultados são alcançados a partir de *inputs* específicos pode ser uma tarefa extremamente complexa.

O ambiente digital automatizado e telemático apresenta particularidades que intensificam a exposição dos indivíduos a riscos técnicos. Diante da complexidade dos sistemas computacionais, das infraestruturas de rede e das técnicas avançadas de processamento de dados, os usuários, em sua maioria, não possuem conhecimento especializado para compreender integralmente os mecanismos que regem a coleta, o armazenamento e o tratamento de suas informações. A crescente

[82] Artigo 27.o
[83] Artigo 26.º.

digitalização das interações, impulsionada pelas plataformas digitais, pela massificação do uso de dados e pelo avanço da inteligência artificial, amplia essa condição de vulnerabilidade, tornando os titulares de dados mais suscetíveis a práticas tecnológicas cuja transparência nem sempre é acessível ao público leigo.[84]

Assim, o titular dos dados ocupa uma posição fragilizada, marcada por uma relação desigual em face do responsável pelo tratamento. Geralmente, o tratamento de dados pessoais é impulsionado por interesses econômicos, seja pela geração direta de lucro, seja pela redução de custos ou aumento de eficiência, muitas vezes de forma discreta e quase imperceptível pelo usuário.

Por outro lado, o titular encontra-se exposto a operações de tratamento que podem invadir sua esfera jurídica, frequentemente sem que ele tenha qualquer conhecimento sobre elas. Durante todas as etapas desse processo informações que pertencem ao titular são passíveis de análise para a criação de perfis baseados em deduções e correlações, as quais servirão de base para decisões posteriormente. Em geral, o indivíduo impactado pela decisão não tem clareza sobre os motivos que a embasaram.[85] Daí a importância do princípio da transparência no tratamento de dados pessoais obtidos na internet, que deve ser colocado em prática e fiscalizado pelas autoridades competentes.

Pasquale defende o uso de auditores que tenham acesso ao algoritmo de modo a garantir que as classificações sejam não-discriminatórias, de modo a combater a opacidade intencional[86]. Ademais, a educação computacional faz-se necessária para um melhor entendimento do que se passa com os dados pessoais.

---

[84] MARQUES, Claudia Lima; MUCELIN, Guilherme. "Vulnerabilidade na era digital: um estudo sobre os fatores de vulnerabilidade da pessoa natural nas plataformas, a partir da dogmática do Direito do Consumidor." Civilistica.com, Rio de Janeiro, v. 11, n. 3, p. 1–30, 2022. p.8.

[85] COSTA, Inês. A proteção de dados pessoais no contexto da União Europeia. Revista Electrónica de Direito, n.º 1, v. 24, fev. 2021, p. 65-66.

[86] PASQUALE, Frank. The Black Box Society.

Considerações finais

Embora a transparência seja fundamental para um meio digital seguro, sua implementação enfrenta desafios significativos, especialmente em um contexto marcado por tensões entre direitos fundamentais e práticas de vigilância. Faz-se, então, necessário um equilíbrio cuidadoso entre a proteção da privacidade e a promoção da transparência para garantir a confiança dos usuários.

Buscou-se demonstrar no presente artigo que a concretização do princípio da transparência no tratamento de dados pessoais na internet manifesta-se por meio da clara comunicação das práticas de coleta, uso e armazenamento de dados. Especialmente nas práticas algorítmicas, as plataformas digitais devem disponibilizar políticas de privacidade acessíveis e compreensíveis, indicando explicitamente quais informações são coletadas, com que finalidades e por quanto tempo serão mantidas. Além disso, deve ser garantido o direito dos usuários de acessar, corrigir e excluir seus dados de forma simples e eficaz. Essas medidas asseguram que os indivíduos possam tomar decisões informadas sobre o compartilhamento de suas informações pessoais online.

Ao longo do estudo, foram apontadas diversas convergências entre a LGPD e o RGPD com relação à transparência e à proteção de dados pessoais, porém, com relação às decisões automatizadas nota-se uma divergência relevante: enquanto o modelo europeu preza pela intervenção humana prévia como salvaguarda, o modelo brasileiro estabelece a revisão posterior como forma de contestação. Essa distinção regulatória reflete visões diferentes sobre o equilíbrio entre a inovação tecnológica e o direito à proteção dos dados pessoais.

A falta de transparência sobre como algoritmos processam os dados e a lógica por trás de perfis automatizados e decisões baseadas em IA não podem ser normalizadas, nas suas diferentes formas de apresentação. Desafios podem ser mitigados através da educação digital, promovendo a conscientização dos usuários sobre seus direitos e práticas de privacidade. No âmbito da criação dos algoritmos, deve haver o

fomento para que o *design* das ferramentas respeitem a privacidade desde a concepção. E, através de fiscalização e auditorias, deve haver a garantia do cumprimento das disposições legais mencionadas ao longo do artigo.

Referências Bibliográficas

ABRANTES, Paula Cotrim de. "Desafios e dilemas da proteção de dados pessoais na era da cultura algorítmica." In: *SciELO Preprints*. DOI 10.1590/SciELOPreprints.7141. p. 1-27, 2023. Disponível em: https://preprints.scielo.org/index.php/scielo/preprint/view/7141 Acesso em 08 jan 2025.

BARBOSA, Sandra. "A importância da transparência e explicabilidade no uso de decisões automatizadas pelo artigo 22.º do RGPD." *Cadernos de Proteção de Dados da União Europeia*, Lisboa: CEDIS, Faculdade de Direito da Universidade Nova de Lisboa, 2022.

BERTOLLI, Emilia. "Os riscos dos testes genéticos." *Varonis*, 2023. Disponível em: https://www.varonis.com/pt-br/blog/os-riscos-dos-testes-geneticos. Acesso em: 20 jan. 2025.

BEZERRA, Daniel Teixeira; FURTADO, Gabriel Rocha. "A (in)constitucionalidade da Medida Provisória n.º 954/2020: o marco jurisprudencial brasileiro do direito fundamental à proteção de dados pessoais." *Civilistica.co*m, Rio de Janeiro, v. 12, n. 1, p. 1–13, 2023. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/849. Acesso em: 6 fev. 2025.

BRANCO, Sérgio; TEFFÉ, Chiara de (coord.). *Plataformas digitais e proteção de dados pessoais*. Rio de Janeiro: ITS – Instituto de Tecnologia e Sociedade, 2023. (Diálogos da pós-graduação em direito digital). Disponível em: https://itsrio.org/wp-content/uploads/2016/12/20231023_Livro_Pos_ITS-UERJ_Plataformas-digitais-protecao-de-dados_COMPLETO.pdf. Acesso em: 11 jan. 2025.

BURRELL, Jenna. "How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, v. 3, n. 1. SAGE Publications, 2016.

CASTELLUCCIA, Claude; MÉTAYER, Daniel Le. "Understanding algorithmic decision-making: Opportunities and challenges." *European Parliamentary Research Service,* 2019. Disponível em: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2019)624261. Acesso em: 31 jan 2025.

COSTA, Inês. "A proteção de dados pessoais no contexto da União Europeia." *Revista Electrónica de Direito*, n.º 1, v. 24, fev. 2021

CORDEIRO, A. Barreto Menezes. *Direito da proteção de dados: à luz do RGPD e da Lei n.º 58/2019.* Coimbra: Almedina, 2022.

CLARKE, Roger; GREENLEAF, Graham**.** "Dataveillance Regulation: A Research Framework*." UNSW Law Research Series*, 7 nov. 2017. Disponível em: https://ssrn.com/abstract=3073492. Acesso em: 20 jan. 2025.

FICO, Bernardo de Souza Dantas; NÓBREGA, Henrique Meng. "The Brazilian Data Protection Law for LGBTQIA+ People: Gender identity and sexual orientation as sensitive personal data" *Revista Direito e Práxis*, v. 13, n. 2, p. 1262–1288, 2022.

DEVILLÉ, Rembrandt; SERGEYSSELS, Nico; MIDDAG, Catherine. Basic Concepts of AI for Legal Scholars. In: BRUYNE, Jan De; VANLEENHOVE, Cedric (ed.). **Artificial Intelligence and the Law**. Antuérpia: Intersentia, 2021. p. 1-22.

DONEDA, Danilo. "O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS." In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coord.). *Direito digital*: direito privado e internet. 3. ed. Indaiatuba: Editora Foco, 2020. pp.33-49.

FÁCIO, Rafaella Nátaly. "A transparência e o direito de acesso no tratamento de dados pessoais: considerações sobre intersecções entre Lei Geral de Proteção de Dados e Lei de Acesso à Informação no Brasil." *Rev. Eurolatin. de Derecho Adm*., Santa Fe, v. 10, n. 2, e247, jul./dic. 2023.

FERNANDES, Micaela Barros Barcelos; OLIVEIRA, Camila Helena Melchior Baptista de. "O artigo 20 da LGPD e os desafios interpretativos ao direito à revisão das decisões dos agentes de tratamento pelos titulares de dados." *Revista de Direito e as Novas Tecnologias*. V.8/2020, jul.-set./2020

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coords.). *Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro*. São Paulo: Thomson Reuters Brasil, 2019

FLUMIGNAN, Silvano José Gomes; FLUMIGNAN, Wévertton Gabriel Gomes. "Princípios que Regem o Tratamento de Dados no Brasil." In: LIMA, Cíntia Rosa Pereira de (Coord.) *Comentários à Lei Geral de Proteção de Dados: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019*. São Paulo: Almedina, 2020.

GOODMAN, Bryce; FLAXMAN, Seth. European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation". *AI Magazine*, v.

38, n. 3, p. 50-57, 2017. Disponível em: https://ojs.aaai.org/aimagazine/index.php/aimagazine/article/view/2741. Acesso em: 10 ago. 2025.

HOOFNAGLE, Chris Jay; SOLTANI, Ashkan; GOOD, Nathan; WAMBACH, Dietrich James; AYENSON, Mika D. "Behavioral Advertising: The Offer You Cannot Refuse." *Harvard Law & Policy Review*, vol.6, n. 273, 2012. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2137601

KHAN, Lina. "What makes tech platforms so powerful. Digital Platforms and Concentration." *Second Annual Antitrust and Competition Conference Stigler Center for the Study of the Economy and the State University of Chicago Booth School of Business*. A Pro-Market Production. 2018. p. 14.

LUCCA, Newton De, MACIEL, Renata Mota. "A PROTEÇÃO DOS DADOS PESSOAIS NO BRASIL A PARTIR DA LEI 13,709/2018: EFETIVIDADE?" In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coord.). *Direito digital: direito privado e internet.* 3. ed. Indaiatuba: Editora Foco, 2020. pp.211-228.

MACHADO, Diego. *Algoritmos e Proteção de Dados Pessoais*. São Paulo: Almedina, 2023. *E-book.* ISBN 9786556279602.

MAGALHÃES, Filipe. *Manual RGPD*. Ordem dos Contabilistas Certificados (OCC), 2018. Disponível em: https://www.occ.pt/fotos/editor2/rgpd--fmagalhaesmanual.pdf. Acesso em: 11 jan. 2025.

MARQUES, Cláudia Lima; MUCELIN, Guilherme. "Vulnerabilidade na era digital: um estudo sobre os fatores de vulnerabilidade da pessoa natural nas plataformas, a partir da dogmática do Direito do Consumidor." *Civilistica.com*, Rio de Janeiro, v. 11, n. 3, p. 1–30, 2022. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/872. Acesso em: 5 jan. 2025.

MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? Rio de Janeiro: Instituto Igarapé, 2018. 27 p. (Artigo Estratégico, 39). Disponível em: https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao--de-Dados-no-Brasil.pdf Acesso em 10 jan. 2025.

Organisation for Economic Co-operation and Development (OECD). "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", *OECD Publishing*, Paris, 2002 https://doi.org/10.1787/9789264196391-en.

O'NEIL, Cathy. *Weapons of math destruction: how big data increases inequality and threatens democracy*. New York: Crown Publishing Group, 2016.

PASQUALE, Frank. *The Black Box Society: The Secret Algorithms that Control Money and Information*-. Cambridge: Harvard University Press, 2015.

PUNIT BHATIA. *Intro to GDPR : A Plain English Guide to Compliance*. Zagreb, Croatia: Advisera Expert Solutions Ltd, 2018. Disponível em: https://research.ebsco.com/linkprocessor/plink?id=15c0c5c9-ff48-39f7-8af6-e648dbb1ae5a. Acesso em: 12 jan. 2025.

RIBEIRO, Elieser. "A potência dos dados para a inteligência artificial." *Medium*, 17 ago. 2020. Disponível em: https://medium.com/@elieser_ribeiro/a-pot%C3%AAncia-dos-dados-para-a-intelig%C3%AAncia-artificial-703f1c05750f. Acesso em: 21 jan. 2025.

ROWLAND, Diane; MACDONALD, Elizabeth; OVERTON, Andrew Charles. *Information technology law*. 3rd ed. London: Cavendish Publishing, 2005.

RUIZ, Evandro Eduardo Seron. Anonimização, pseudonimização e desanonimização de dados pessoais. In: LIMA, Cíntia Rosa Pereira. *Comentários a Lei Geral de Proteção de Dados – Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019.* São Paulo: Almedina Brasil, 2020.

SCHLOTTFELDT, Shana. "REVISÃO DE DECISÃO TOMADA COM BASE EM TRATAMENTO AUTOMATIZADO: PREOCUPAÇÕES E CONSIDERAÇÕES SOBRE A EFETIVAÇÃO DA TRANSPARÊNCIA PARA COBRIR A DISCRIMINAÇÃO ALGORÍTIMICA E O PROFILING." In: MENDES, Laura Schertel Ferreira (Org.) et al. *Anuário do Observatório da LGPD da Universidade de Brasília: análise comparada entre elementos da LGPD e do GDPR*. Brasília: Universidade de Brasília, Faculdade de Direito, 2024. 2 v. pp. 117-136

SUNYAEV, Ali. *Internet Computing: Principles of Distributed Systems and Emerging Internet-Based Technologies.* Cham: Springer, 2020.

WANDERER, Bertrand. "Economia movida a dados e o papel das plataformas digitais." *Journal of Law and Regulation*, v. 9, n. 2, p. 22–43, 2023. Disponível em: https://periodicos.unb.br/index.php/rdsr/article/view/43231. Acesso em: 6 fev. 2025.