CAPÍTULO 4

A PROBLEMÁTICA DA VENDA DE ÍRIS E O CONSENTIMENTO INFORMADO À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS

https://doi.org/10.22533/at.ed.8192523094

Luísa Scolari Corrêa
Bacharela em Direito pela Fundação Escola Superior do Ministério Público (FMP/RS). Advogada

RESUMO: O presente artigo busca analisar a comercialização de íris proposta por empresas privadas em troca de criptomoedas à luz da Lei Geral de Proteção de Dados e demais normas do ordenamento jurídico brasileiro, considerando a natureza dos dados objeto de comércio e a base legal do consentimento informado utilizado. A pesquisa se sustentou no exame de artigos legais das normativas pontuadas e no Projeto de Lei nº 36/2025, além de decisões e da doutrina sobre a temática, somada à verificação das peculiaridades em que o caso concreto se deu. A conclusão da pesquisa apontou para a violação ao direito à intimidade e à privacidade, culminando ao indevido vazamento de dados sensíveis em prol da ambiência mercadológica, em virtude de tratamento realizado em violação direta ao consentimento informado, considerando que esse exige requisitos - livre, informado e inequívoco - que não restaram contemplados.

THE PROBLEM OF IRIS SALE AND INFORMED CONSENT IN LIGHT OF THE GENERAL DATA PROTECTION LAW

ABSTRACT: This article aims to analyze the commercialization of irises proposed by private companies in exchange for cryptocurrencies, in light of the General Data Protection Law and other norms of the Brazilian legal system, considering the nature of the data involved in the trade and the legal basis of the informed consent used. The research was based on the examination of legal articles of the relevant regulations, Law Project nº 36/2025, as well as decisions and doctrine on the subject, combined with an analysis of the specific circumstances of the case. The conclusion of the study pointed to a violation of the right to intimacy and privacy, culminating in the improper leakage of sensitive data for market purposes, due

to processing carried out without a legal basis currently in place. It is important to note that informed consent requires specific conditions—free, informed, and unequivocal—which were not met in this case.

INTRODUÇÃO

Não se desconhece a crescente evolução da tecnologia e o recrudescimento de um mundo cada vez mais virtual. Esses gradativos e exponenciais avanços permitiram diversas facilidades para a sociedade de forma geral, pois garantiram maior comunicação e dinamismo, pontos que só enriqueceram o movimento de globalização. Dessas e de outras consequências do desenvolvimento tecnológico foi possível realizar mais ações em um menor período, otimizando o tempo e acelerando as atividades corriqueiras ordinárias da vida em sociedade.

Essa atual conjuntura é destacada pela doutrina de Felipe Peixoto Braga Netto, Cristiano Chaves de Farias e Nelson Rosenvald (2019, pág. 933):

> "A Internet torna comum, global, partilhado o que nela está. Não há fronteiras entre países, não há limitações geográficas. As relações na dimensão digital são dinâmicas, os conteúdos emergem de recíprocos contatos colaborativos. Rompem-se, da mesma forma, muitas barreiras culturais, aproximando-se os povos - que estão à distância de um clique, não mais dependendo dos modos convencionais de contato.
>
> Somos todos, hoje, em maior ou menor medida, dependentes do mundo digital. [...]."

Mais ainda, os autores ainda destacam a intensa troca de informações a partir do alargamento da tecnologia (2019, pág. 931):

> "Não é exagero afirmar que vivemos na era da informação. Se os instrumentos técnicos (*smartphones, tablets etc.*) que propiciam o compartilhamento das informações se renovam e se sucedem em pouco tempo, com a mais recente tecnologia substituindo as que pensávamos serem as últimas novidades, há, em tudo isso, uma permanência: a intensa e irreversível troca - quase imediata - de informações. Esse intercâmbio de informações, sem precedentes na história humana, mudou, de muitos modos, o perfil da nossa sociedade. [...]. As empresas privadas, os governos, as pessoas em geral, mostram-se sensíveis em relação ao que é dito sobre elas nas redes sociais, porque são elas, as redes sociais, até mais do que os veículos convencionais, que parecem formar a convicção social sobre determinados temas."

Corolário a esse movimento global, o mundo jurídico foi instigado a buscar maior proteção aos concretos e sedimentados direitos fundamentais, que se mostraram ameaçados em meio àquilo que parecia ser algo irrefreável. Indubitavelmente, uma das primeiras e principais regulamentações foi a Lei nº 12.965/2014, o Marco Civil da Internet, seguida mais recentemente pela Lei nº 13.709/2018, a Lei Geral de Proteção de Dados. Em relação a esta última, houve o aprimoramento do conceito de dados pessoais e sua classificação, mas foi apenas com a Emenda Constitucional nº 115 de 2022 que a proteção dos dados pessoais tornou-se um direito fundamental.

Contextualizado o movimento da evolução tecnológica, é salutar destacar a importância da elevação da proteção dos dados pessoais ao rol - aberto - de direitos fundamentais. Nota-se que o legislador não a fez por acaso, mas obedeceu ao significado que tais direitos foram adquirindo ao longo do tempo com a tecnologia e a inovação. Isso porque os dados pessoais ganharam valor - inclusive econômico - à medida que consagraram informações únicas de cada indivíduo - a exemplo do número de CPF ou RG, endereço eletrônico ou domiciliar, entre outros - que possibilitam a identificação e a constituição de relações que, por vezes, sequer o titular dos dados tem conhecimento - o que acaba por violar o regramento brasileiro, conforme se verá adiante.

A relevância da proteção dos dados pessoais como direito fundamental é tema de extrema complexidade, à qual Zanatta aborda com maestria (2024, páginas 216 e 217):

> "A proteção de dados pessoais possui um conjunto de finalidades teleológicas, concebidas em uma teoria política democrática. Ela não é um fim em si mesmo, mas busca fazer avançar certos tipos de ideais democráticos, como os direitos de liberdade, de devido processo, de igualdade e de redução de desigualdades entre pessoas, que devem ser tratadas com dignidade.
>
> [...]
>
> O direito de proteção de dados pessoais não é a mesma coisa que o direito de privacidade. Como ponto de partida, deve-se considerar que a privacidade é um dos componentes normativos da proteção de dados pessoais, mas não se confunde com ela. A proteção de dados pessoais busca avançar outros ideais normativos, como o livre desenvolvimento da personalidade, a redução das assimetrias de poder, a equidade e não discriminação, e as cláusulas assecuratórias de liberdade, em sentido amplo."

A crescente valorização dos dados pessoais e sua consequente proteção também se deu porque, em plena sociedade da informação, com dados sendo transmitidos constantemente e publicizados a todo o momento, verificou-se o aumento no número de fraudes e de utilização indevida de informações atinentes a terceiros que, no mínimo, violam a intimidade e a privacidade dos seus titulares. O enaltecimento, por conseguinte, veio à tona para tentar resgatar o controle dos dados pessoais ao seu titular, como verdadeiro resultado a evitar e a combater a prática de infrações civis ou penais com informações únicas e particulares de terceiros.

Nessa sistemática, a Lei Geral de Proteção de Dados intitulou como dados sensíveis aqueles que dizem respeito *à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural* (art. 5º, inciso II, da LGPD), o que garante ao titular ainda mais segurança quanto à sua divulgação, exigindo maior proteção quando comparados aos dados pessoais "não sensíveis", restringindo com mais rigor a possibilidade de publicização daqueles. A partir dessa conjuntura, a referida Lei elencou algumas bases legais a permitir eventual tratamento de dados, isto é,

qualquer operacionalização com os dados, seja a coleta, produção e recepção, seja classificação, utilização, acesso, reprodução, transmissão e distribuição (art. 5º, inciso X), a fim de recrudescer a regulamentação e o monitoramento dessas informações.

Outrossim, com o fito de nortear a aplicação dos dados pessoais, a Lei Geral de Proteção de Dados arrolou diversos fundamentos que devem ser observados, sendo pertinente destacar a *autodeterminação informativa, o respeito à privacidade, a garantia da liberdade de expressão, de informação, de comunicação e de opinião e a inviolabilidade da intimidade, da honra e da imagem* (art. 2º). Tais diretrizes buscam preservar a utilização dos dados pessoais de forma harmônica às suas finalidades e ao ordenamento jurídico protetivo.

Outrossim, segundo consta no art. 7º da Lei Geral de Proteção de Dados[1], *o tratamento de dados pessoais somente poderá ser realizado* nas hipóteses restritas, elencadas à Lei, sendo uma delas o *fornecimento de consentimento pelo titular.* Isso significa que o tratamento de dados não pode ser feito de forma discricionária e a concordância do titular é uma das formas a permitir a realização de alguma operação com esses dados. Contudo, a referida base legal foi conceituada no próprio Diploma Legal supra ao dispor consentimento como *manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.* Veja-se, portanto, que a Lei acabou por determinar requisitos necessários para o preenchimento da citada base legal, não sendo suficiente qualquer consentimento apresentado.

Sendo assim, diante dessa exposição, cabe aqui avaliar o tema central a que se propôs este artigo, qual seja, a venda da íris para empresas privadas. Por primeiro, é inegável que as informações constantes no desenvolvimento da íris contém dados genéticas - mais especificamente cerca de 2.000 genes, sendo que 50 deles afetam os padrões (ANCESTRY, pág. 3) -, o que resta clara a sua possibilidade de enquadramento no conceito de dados pessoais sensíveis. Em consectário lógico, tais dados requerem maior proteção, sendo que eventuais bases legais utilizadas devem constar expressamente presentes e se mostrarem claras, a fim de garantir que o tratamento realizado não burle a sistemática protetiva.

[1] São arroladas outras bases legais, como: II - para o cumprimento de obrigação legal ou regulatória pelo controlador;III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) VigênciaIX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente

Com o objetivo de aprofundar o estudo da temática proposta, impõe-se a análise do caso em que se deu a comercialização dos dados sensíveis elencados.

CASO CONCRETO

Segundo noticiado (CNN Brasil, 2025), a empresa Tools for Humanity (TfH) estabeleceu mais de 50 pontos de coleta na cidade de São Paulo e passou a escanear a íris de pessoas em troca do pagamento de 48 criptoativos, o que pode equivaler cerca de 500 reais, a depender da cotação diária. O objetivo, conforme informações apresentadas pela empresa e divulgadas pela mídia, seria a de criar uma documentação mundial ("World ID") a fim de *obter um código único que não pode ser reproduzido pela inteligência artificial* (CNN Brasil, 2025). O projeto foi idealizado por Sam Altman, CEO da OpenAI, que referiu que *a ideia é diferenciar humanos de robôs e inteligências artificias, com cada usuário humano tendo uma World ID, espécie de "passaporte" que serve como uma "prova de humanidade"* (VEJA, 2025).

Ainda de acordo com o divulgado, a empresa teria relatado que não fica com os dados dos usuários e que, em 29 de janeiro de 2025, cerca de 500 mil pessoas já teriam fornecido sua íris nos pontos de coleta. O procedimento, nos termos em que publicado, inicia-se pelo *download* do aplicativo, seguido pelo aceite dos termos e condições propostas, sendo que a divulgação do nome e do telefone é opcional. Após isso, marca-se um horário nos centros de coleta, local onde as pessoas se dirigem para fornecer seus dados constantes em sua íris e receber a contrapartida (CNN Brasil, 2025).

Para melhor compreensão da sistemática de coleta utilizada, a revista Veja buscou sintetizou o que a empresa descreveu em nota (VEJA, 2025):

> "Em nota, a World diz que 'nenhum pagamento é oferecido aos usuários' e que 'não fica com nenhum dado das pessoas que se verificam como humanos únicos'. Segundo a empresa, "o processo funciona como um como um dispositivo de última geração chamado Orb, que captura uma imagem do olho e do rosto, que é imediatamente convertida por algoritmos em uma representação numérica chamada de código de íris. As magens originais da íris são então criptografadas de ponta-a-ponta, enviadas para o telefone da pessoa e prontamente deletadas da Orb, e o código de íris é então fracionado por meio de criptografia avançada, conhecida como Computação Multi-partidária Anonimizada (AMPC). Os fragmentos são armazenados em nós computacionais operados por universidades e terceiros confiáveis, como as Universidades de Berkeley nos EUA e Friedrich Alexander Erlangen-Nürnberg, na Alemanha. Os fragmentos criptografados não revelam nada sobre o indivíduo nem podem ser efetivamente vinculados de volta a ele. A World assegura a efetiva anonimização dos dados".

Ocorre que diversas problemáticas decorreram dessa situação. Pelo informado, brasileiros que tiveram sua íris escaneada referiram dificuldades para resgatar os valores prometidos no aplicativo (G1, 2025). Segundo os participantes, o aplicativo

é o meio para o passo inicial do projeto e também o local onde o pagamento fica armazenado. Mais ainda, há informações de que o aplicativo não está redigido totalmente em língua portuguesa, mesclando idiomas, apresentando conteúdo até em língua espanhola, o que dificulta a compreensão dos usuários.

Não o suficiente, os participantes reclamaram da falta de esclarecimentos, referindo que alguns receberam em contrapartida apenas uma parcela de R$ 24,00, enquanto outros receberam R$ 300,00, o que levou especialistas a concluírem pela violação ao direito dos consumidores, dada a ausência de informações claras e precisas (G1, 2025).

Ao decorrer desses fatos, a Autoridade Nacional de Proteção de Dados, por meio do seu Conselho Diretor, proferiu decisão que manteve a suspensão da compensação financeira realizada pela escaneamento de íris para identidades digitais, em criptomoedas ou outra forma de pagamento (ANPD, 2025). Na ocasião, a Autoridade Nacional indeferiu o pedido da empresa para concessão de prazo adicional para implementação de mudanças no aplicativo.

No que atine ao mérito da decisão cautelar, a relatora Miriam Wimmer enfatizou que a contraprestação pecuniária teria o condão de invalidar o consentimento e a autodeterminação informativa, nos seguintes termos:

> "[...] na hipótese concreta, a coleta de íris vinculada à referida compensação financeira teria o potencial de invalidar o livre consentimento, o que contraria o disposto na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018 – LGPD) e põe em risco o direito fundamental à proteção de dados pessoais dos titulares que eventualmente se submetem ao procedimento de coleta da íris.
>
> [...]
>
> Para ser válido, o consentimento deve ser livre, informado e inequívoco, conforme previsto no art. 5º, XII, da LGPD. Para fins do presente voto, é necessário avaliar, especialmente, se o consentimento obtido pela TFH para a coleta de dado sensível biométrico (íris), mediante contrapartida financeira, atende ao qualificativo "livre"."

In casu, a relatora ainda discorreu sobre a gravidade diante do vício no consentimento, precipuamente pelo qualidade dos dados coletados, senão vejamos:

> "O risco decorrente do vício do consentimento no caso em análise é ainda maior considerando-se que o serviço ofertado pela recorrente se baseia: (i) em uma tecnologia emergente e inovadora, cujos efeitos ainda não são plenamente conhecidos, tendo sido objeto de questionamentos por autoridades de proteção de dados e tribunais em diversas regiões do mundo; (ii) na coleta da íris, dado biométrico de natureza sensível, ao qual é conferida especial proteção pela LGPD, incluindo a expressa atribuição de competência a ANPD para regulamentar ou vedar "a comunicação ou o uso compartilhado de dados pessoais sensíveis com o objetivo de obter vantagem econômica" (art. 11, § 3º); e (iii) em um procedimento caracterizado por sua irreversibilidade, seja em razão do caráter único da íris (informação pessoal que, ao contrário de uma senha, por exemplo, não pode ser alterada pelo titular), seja em razão do registro dessas informações por meio da tecnologia blockchain, que, por padrão, impede a sua modificação ou exclusão."

Em vista disso, apresentado o panorama em que se deu o caso em análise, impende avaliar o conceito da base legal do consentimento informado e suas implicações no deslinde da temática.

FRAGILIDADE DA BASE LEGAL DO CONSENTIMENTO INFORMADO E SEUS REQUISITOS

Conceituado à Lei de Proteção de Dados, o consentimento é *a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada* (art. 5º, XII). Apenas por essa definição, já é possível extrair que para a existência de consentimento válido é necessária que a declaração seja ***livre, informada e inequívoca*** e com o ***propósito determinado.***

Veja-se que, figurando como base legal para um direito agora fundamental - proteção de dados pessoais - e intimamente relacionado com ao menos um dos fundamentos da Lei Geral de Proteção de Dados - a autodeterminação informativa -, o consentindo deve ser interpretado de forma a garantir uma segura e concreta expressão humana que efetivamente aponte para o seu assentimento, preenchendo os requisitos elencados e apontando para certa e - conhecida - finalidade.

Neste ponto, acerca da forma como a interpretação do direito fundamental à proteção de dados deve se dar, circundada pela base legal do consentimento - quando esta é a elencada -, discorre o professor Ingo Sarlet (2022, páginas 32 à 34):

> "Assim, uma compreensão/interpretação/aplicação constitucionalmente adequada do direito fundamental à proteção de dados deverá sempre ser pautada por uma perspectiva sistemática, que, a despeito do caráter autônomo (sempre parcial), desse direito, não pode prescindir do diálogo e da interação (por vezes marcada por concorrências, tensões e colisões) com outros princípios e direitos fundamentais, que, dentre outros pontos a considerar, auxiliam a determinar o seu âmbito de proteção, inclusive mediante o estabelecimento de limites diretos e indiretos.
>
> De particular relevância no caso brasileiro - justamente pela existência, além da nova LGPD e de outras leis que versam sobre o tema, é ter sempre presente que, impõe-se ao Estado (...), por força de seus deveres de proteção, não apenas zelar pela consistência constitucional do marco normativo infraconstitucional (inclusive da LGPD) no tocante aos diplomas legais isoladamente considerados, mas também de promover sua integração e harmonização produtiva, de modo a superar contradições e assegurar ao direito fundamental à proteção de dados, sua máxima eficácia e efetividade.
>
> Um dos aspectos a destacar (...) é que de acordo com o entendimento do Supremo Tribunal Federal brasileiro, o direito fundamental à proteção de dados pessoais assume a condição de direito fundamental autônomo, o que significa que a despeito de sua íntima conexão com outros princípios e direitos fundamentais (com destaque para a autodeterminação informacional e o direito à privacidade), com esses não se confunde, porquanto possui um âmbito próprio e reservado de proteção, ademais de um núcleo essencial."

No mesmo sentido, o Superior Tribunal de Justiça, no julgamento do Recurso Especial nº 2121904/SP, debruçou-se sobre a temática ao balizar alguns princípios que norteiam a proteção de dados, precipuamente em relação à sua necessária finalidade:

> "17. Sobre o tema, destaca-se o princípio da finalidade, segundo o qual o tratamento de dados deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades (art. 6º, I). 18. O princípio da adequação, por sua vez, preceitua que deve existir compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento (art. 6º, II). 19. Ainda, incide o princípio da transparência, que garante aos titulares, informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial (art. 6º, VI)."

É, pois, nessa ambiência que se dá o consentimento informado. Note-se que, com o objetivo de concretizar o exercício do direito fundamental à proteção de dados, tal base legal, caso utilizada, deve-se preservar a significância e a altura que representa os dados tratados, principalmente quando se está diante de dados sensíveis, como mostra o caso em concreto. Não à toa, pois, que no mesmo julgamento supracitado, a Corte Superior entendeu que quando se trata de vazamento de dados pessoais sensíveis, os danos são presumidos, dada a gravidade e a relevância das informações compartilhadas[2].

Especificamente em relação à forma em que se deve colher o consentimento, é preciso observar que a manifestação genérica não se mostra válida. Neste ponto, refere Paulo Khouri (2021):

> "Ou seja, não basta dizer o "aceito" ou "li e concordo" [remetendo aos termos de uso apresentados pelas plataformas digitais]. Em sintonia com a GPDR, é preciso que esse consentimento seja livre, informado e inequívoco. De forma expressa, a LGPD veda consentimentos genéricos: é o chamado "consentimento informado livre e esclarecido". Não é o mero consentir, é o consentir qualificado. É o consentir que não autoriza consentimentos genéricos: tem que ser livre, informado e inequívoco. [...] Pode-se dizer que, sem o cumprimento das condições impostas pelo inciso XII do artigo 5º, não há consentimento válido."

Dito isso, é possível observar que o consentimento informado deve representar verdadeira liberalidade do titular de dados quanto ao seu tratamento, e sua interpretação deve ocorrer de forma restritiva (Tepedino e Teffé, 2020), vinculada diretamente aos requisitos elencados à Lei.

No caso em apreço, verifica-se de pronto que os requisitos para o consentimento válido não foram observados. Segundo a empresa, o consentimento foi respeitado quando os participantes se dispuseram a fornecer seus dados e se dirigiram aos

[2] Informação que se verifica na seguinte passagem da decisão: "29. Decidiu, então, que o vazamento de dados pessoais comuns, "a despeito de se tratar de falha indesejável no tratamento de dados de pessoa natural por pessoa jurídica, não tem o condão, por si só, de gerar dano moral indenizável. Ou seja, o dano moral não é presumido, sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações". 30. Por outro lado, registrou que "diferente seria se, de fato, estivéssemos diante de vazamento de dados sensíveis, que dizem respeito à intimidade da pessoa natural", hipótese em que, na visão da Segunda Turma, seria possível o dano presumido"

centros de coleta (ANPD, 2025). Todavia, conforme bem apontado pela Autoridade Nacional na decisão que manteve a suspensão do projeto, a participação das pessoas envolvia uma contrapartida, o que inevitavelmente maculou a base legal indicada (2025, página 12):

> No caso em análise, a empresa argumentou que o consentimento dos Titulares "[é] o reflexo da expressão da vontade de ser um participante de um projeto global de criação de uma identidade única". No entanto, há evidências de que Titulares anuem com o tratamento de seus dados biométricos única e exclusivamente em razão da compensação financeira e não, como argumenta a recorrente, para participar "de um projeto global de criação de uma identidade única". Como amplamente noticiado, muitas pessoas "não sabiam explicar do que se tratava o protocolo World e nem se havia riscos". Um dos entrevistados disse à reportagem do G1 o seguinte: "eu vim pelo dinheiro mesmo. Estou duro. Mas nada é de graça, né?" (...)".

Em relação a esta ambiência mercadológica, Tepedino e Teffé já alertavam acerca do perigo em conceder eventual caráter comercial ao consentimento (páginas 11 e 12, 2020):

> "O consentimento representa instrumento de manifestação individual no campo dos direitos da personalidade e tem o papel de legitimar que terceiros utilizem, em alguma medida, os dados de seu titular.29 Ele compreende a liberdade de escolha, sendo meio para a construção e delimitação da esfera privada. Associase, portanto, à autodeterminação existencial e informacional do ser humano, mostrando-se imprescindível à proteção do indivíduo e à circulação de informações.
>
> **Nessa direção, mostra-se inadequado atribuir natureza negocial ao consentimento, visto que tal entendimento reforçaria o sinalagma entre o consentimento e determinada vantagem econômica obtida por aquele que consente – a reforçar indesejada índole patrimonial e de fomento à utilização de esquemas proprietários para o trato dos dados pessoais**" - *grifei*

Contudo, a violação ao direito fundamental referente à proteção de dados não se esgota apenas no vício referente à liberalidade da participação no projeto. Nota-se, ainda, que as próprias informações referentes à finalidade da coleta desses dados restou prejudicada, tendo em vista que o propósito de *criação de uma identidade única*, por si só, não preenche o requisito sobre o seu intuito finalístico. Isso porque a empresa não apresentou a forma como se daria o tratamento, nem mesmo o motivo pelo qual se propunha a criar a identidade humana única, remanescendo muitas dúvidas sobre como seriam efetivamente utilizadas as informações coletadas. Tais elementos, em verdade, também fazem parte da ideia do consentimento informado.

Não o suficiente, conforme referido no item anterior, diversos problemas ocorreram no aplicativo da empresa, inclusive com contraprestações pecuniárias discrepantes, o que deixou ainda mais nebulosa a proposta, violando a necessária informação aos titulares dos dados.

Em uma perspectiva ideal, seguindo o raciocínio elencado pela Constituição Federal e pela Lei Geral de Proteção de Dados, a Doutrina ainda aponta que o elemento da liberdade integrante da base legal do consentimento pressupõe a

escolha das etapas pelas quais o titular aceita que seus dados sejam tratados, sem precisar consentir "tudo ou nada" (Tepedino e Teffé, 2020). Mas para isso, por claro, será necessário que o titular conheça efetivamente essas fases de operacionalização pelas quais os seus dados irão passar, informações estas que sequer foram apresentadas no caso em análise. É porque a possibilidade de assentimento presume conhecimento, pois, para consentir algo é preciso antes obter informações. Em outras palavras, ninguém possui a capacidade de concordar com algo que desconhece.

Nesse sentido, referem Tepedino e Teffé (2020, páginas 14 e 15):

> "Na lógica do consentimento informado, o art. 9º da LGPD dispõe que 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 da: (I) finalidade específica do tratamento; (II) forma e duração do tratamento, observados os segredos comercial e industrial;41 (III) identificação do controlador; (IV) informações de contato do controlador; (V) informações acerca do uso compartilhado de dados pelo controlador e a finalidade; (VI) responsabilidades dos agentes que realizarão o tratamento; (VII) e direitos do titular, com menção explícita aos direitos contidos no art. 18.42 Na hipótese em que o consentimento é requerido, ele 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. (…)".

Dito isso, considerando os diversos pontos passíveis de discussão acerca da viabilidade do consentimento informado e de seus requisitos, a temática alcançou o Poder Legislativo, culminando no Projeto de Lei nº 36/2025. Tal normativa, ainda que em tramitação, merece ser analisada com a finalidade de se verificar as eventuais novas perspectivas do tema em apreço.

PROJETO DE LEI 36/2025

O tema acerca do consentimento informado é instigante e nem sempre encontra-se atrelado à tentativa de consagrar a proteção de dados. Após a proposta da empresa Tools for Humanity (TfH) se concretizar e as discussões sobre a validade do consentimento informado virem à tona, o deputado Ricardo Ayres apresentou o Projeto de Lei nº 36/2025, a fim de alterar a Lei Geral de Proteção de Dados para *proibir a oferta mediante pagamento de disponibilidade de dados biométricos sensíveis e estabelecer medidas mais rigorosas de proteção a esses dados.* Como justificativa, no entanto, a necessidade de maior proteção aos dados pessoais não se mostrou como o maior enfoque. O parlamentar ponderou, em verdade, a busca em delimitar o que chamou de *proibição ampla e indistinta da oferta de dados biométricos,* a saber:

> "A proibição ampla e indistinta da oferta de dados biométricos, mesmo nos casos em que haja consentimento informado, pleno cumprimento das regras da LGPD e anonimização de dados, compromete não apenas a autonomia privada dos cidadãos, mas também o espaço legítimo de atuação econômica das empresas que operam em setores inovadores como identidade digital, verificação biométrica, fintechs,

> healthtechs e serviços de segurança da informação. Diante disso, é imprescindível que o Projeto de Lei nº 36/2025 seja redistribuído para que as Comissões de Desenvolvimento Econômico (CDE) e de Indústria, Comércio e Serviços (CICS) também se manifestem sobre o mérito da matéria. Ambas possuem competência regimental para avaliar proposições que impactam o ambiente de negócios, a atividade empresarial e os setores produtivos, sendo o foro adequado para que os efeitos econômicos da proposta sejam sopesados à luz dos princípios constitucionais da liberdade econômica e da livre concorrência."

Nota-se, pela análise da justificativa originalmente apresentada, que o projeto de lei nasce com o fito de garantir a segurança jurídica sobre quais hipóteses efetivamente permitem o tratamento de dados sensíveis, mas sobretudo em prol da liberdade econômica e empresarial. Tal motivação, a nosso ver, desvirtua o propósito e a finalidade da Lei Geral de Proteção de Dados, que não ignora a liberdade negocial e de mercado, mas prima pela proteção de dados, essencialmente os sensíveis.

É que, conforme exaustivamente disposto acima, não se deve conceber caráter mercadológico a dados únicos e definitivos, sob pena de violação à autodeterminação e ao consentimento informado.

Entretanto, após a proposta ser aprovada pela Comissão de Constituição e Justiça e Cidadania (CCJC), a justificativa do projeto ganhou outra roupagem. Em seu conteúdo destacam-se a *vedação da comercialização de dados biométricos sensíveis, sob qualquer forma* e a possibilidade de *o titular dos dados, em qualquer momento, mediante manifestação expressa, solicitar o cancelamento e a exclusão de seus dados biométricos sensíveis.* Em relação à motivação propriamente dita, foram apresentados fundamentos que se coadunam com a Lei Geral de Proteção de Dados, pois já iniciou pela necessidade de *fortalecer a proteção dos dados biométricos sensíveis,* esposado nos seguintes termos:

> "A presente proposta visa fortalecer a proteção dos dados biométricos sensíveis, como o reconhecimento da íris, face, voz e DNA, diante do crescente uso dessas tecnologias e dos riscos associados à sua comercialização. Recentemente, práticas como a oferta de pagamento em troca do escaneamento da íris têm ganhado destaque, como reportado pela CNN Brasil (https://www.cnnbrasil.com.br/tecnologia/conheca-o-que-esta-portras-e-os-riscos-de-escanear-a-iris-por-dinheiro/). Essas práticas expõem os cidadãos a riscos significativos, como fraudes, violação de privacidade e uso indevido de dados para fins ilícitos. A Lei Geral de Proteção de Dados (LGPD) já estabelece diretrizes importantes para o tratamento de dados pessoais, mas não proíbe expressamente a comercialização de dados biométricos sensíveis. A ausência de uma proibição clara cria lacunas que podem ser exploradas por empresas e organizações, colocando em risco a privacidade e a segurança dos cidadãos. Dados biométricos são únicos e irreversíveis. Uma vez violados, não há como reverter o dano, pois não é possível alterar características como a íris ou a impressão digital. Além disso, a comercialização desses dados pode facilitar a criação de bancos de dados ilegais, usados para vigilância em massa, discriminação ou até mesmo perseguição política. A proposta também se alinha a princípios internacionais de proteção de dados, como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, que classifica dados biométricos como categorias especiais de dados pessoais, sujeitos a salvaguardas rigorosas. No Brasil, é essencial avançarmos nessa direção, garantindo que a LGPD esteja à altura dos desafios impostos pelas novas tecnologias."

Pelo discorrido, é possível verificar que a exposição de motivos do projeto reconhece consequências graves e muitas vezes irreversíveis do tratamento de dados realizado de forma irregular. Reconheceu-se, ainda, o envolvimento de interesses políticos e negociais que podem ferir e violar o propósito original dos dados pessoais, situação que exige maior atenção, principalmente da Autoridade Nacional de Proteção de Dados.

De todo modo, incumbe destacar que o projeto de lei segue em tramitação, sendo imperioso seu acompanhamento para melhor avaliação do desfecho desse debate.

CONCLUSÃO

Por derradeiro, a par das construções estabelecidas nesta presente pesquisa, a iniciar pela conceituação de dados pessoais sensíveis e pelo significado e importância do consentimento informado válido, sem abandonar a análise da elevação da proteção de dados como direito fundamental, é possível perceber que a comercialização de íris pela empresa Tools for Humanity (TfH) violou a privacidade e a intimidade dos titulares ao tratar dados pessoais sensíveis, ao menos da forma como foi feita, por razões multifatoriais, dentre elas a ausência de informação adequada sobre a finalidade e o procedimento do tratamento de dados e a falta do preenchimento de requisitos para o reconhecimento de consentimento válido. A presente pesquisa possibilitou verificar a profundidade do debate sobre os dados pessoais sensíveis, que definitivamente não podem ser elencados a um ambiente mercadológico e negocial.

Diante do aumento da valoração que os dados pessoais assumiram ao longo do tempo, inseridos em uma "sociedade da informação", a proteção dos dados pessoais, essencialmente os sensíveis, merecem maior respaldo. As características da ambiência mercadológica não podem ofuscar os requisitos e hipóteses que almejam proteger os dados de seus titulares.

REFERÊNCIAS

Braga Netto, Felipe Peixoto; De Farias, Cristiano Chaves; Rosenvald, Nelson. Novo Tratado de Responsabilidade Civil. 4ª edição. São Paulo: Saraiva Educação, 2019.

BRASIL. Lei nº 13.709/2018. Lei Geral de Proteção de Dados. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 28 de maio de 2025.

BRASIL. Lei nº 12.965/2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.Acesso em 31 de maio de 2025.

Zanatta, Rafael. Os sentidos do direito da proteção de dados pessoais: desmembrando a complexidade do direito e dos direitos. In: Amato, Lucas Fucci. (Org). Sociologia do Direito Digital: Inteligência Jurídica na era da Inteligência Artificial. Conselho editorial - Livros Abertos da Faculdade de Direito. São Paulo, 2024.

Ancestry. Centro de Aprendizagem de Traços AncestryDNA. Padrões de Íris. Disponível em: https://www.ancestry.com/c/traits-learning-hub/iris-patterns#:~:text=Gen%C3%A9tica%20do s%20Padr%C3%B5es%20de%20 %C3%8Dris&text=Isso%20os%20torna%20um%20fen%C 3%B3tipo,de%2050%20 afetam%20seus%20padr%C3%B5es. Acesso em 31 de maio de 2025.

Helder, Darlan. G1 Tecnologia. 13 de fevereiro de 2025. Brasileiros pagos para escanear íris enfrentam dificuldades com aplicativo do projeto: 'Perdi a conta e o dinheiro'. Disponível em: https://g1.globo.com/tecnologia/noticia/2025/02/13/brasileiros-pagos-para-escanear-a-iris-en frentam-dificuldades-com-aplicativo-do-projeto-perdi-a-conta-e-o-dinheiro.ghtml. Acesso em 31 de maio de 2025.

Milanezi, Gabriela. CNN Brasil. 29 de janeiro de 2025. Empresa paga cerca de R$500 por escaneamento de íris; entenda como é feito. Disponível em: https://www.cnnbrasil.com.br/nacional/sudeste/sp/empresa-paga-cerca-de-r-500-por-escane amento-de-iris-entenda-como-e-feito/. Acesso em 31 de maio de 2025.

Gil, Radar. Veja Negócios. 17 de janeiro de 2025. Venda de Íris no Brasil? Entenda os riscos do novo projeto de Sam Altman. Disponível em: https://veja.abril.com.br/coluna/radar-economico/venda-de-iris-no-brasil-entenda-os-riscos-d o-novo-projeto-de-sam-altman/. Acesso em 31 de maio de 2025.

Ministério de Justiça e Segurança Pública. Autoridade Nacional de Proteção de Dados. Fiscalização. Após recurso administrativo, Conselho Diretor mantém suspensão de pagamento por coleta de íris. 11 de fevereiro de 2025. Disponível em https://www.gov.br/anpd/pt-br/assuntos/noticias/apos-recurso-administrativo-conselho-diretor-mantem-suspensao-de-pagamento-por-coleta-de-iris. Acesso em 1º de junho de 2025.

BRASIL. Superior Tribunal de Justiça. Terceira Turma. Recurso Especial nº 2121904/SP. PRUDENTIAL DO BRASIL SEGUROS DE VIDA S.A. Recorrido: Pedro Henrique Camilloti. São Paulo. Relatora Ministra Nancy Andrighi. 11 de fevereiro de 2025. Disponível em https://scon.stj.jus.br/SCON/pesquisar.jsp?pesquisaAmigavel=+dados+sens%EDveis+e+gen%E9tico&b=ACOR&tp=T&numDocsPagina=10&i=1&O=&ref=&processo=&ementa=&nota=&filtroPorNota=&orgao=&relator=&uf=&classe=&juizo=&data=&dtpb=&dtde=&operador=e&thesaurus=JURIDICO&p=true&livre=dados+sens%EDveis+e+gen%E9tico. Acesso em 02 de junho de 2025.

Bittar, Eduardo C.B; Sarlet, Gabrielle B. Sales; Sarlet, Ingo Wolfgang. Inteligência Artificial, Proteção de Dados Pessoais e Responsabilidade na Era Digital. Série Direito, Tecnologia, Inovação e Proteção de Dados num Mundo em Transformação. Expressa Jur, 2022.

Khouri, Paulo Roque. 31 de março de 2021. Garantias do Consumo: O problema do consentimento informado na Lei Geral de Proteção de Dados. Consultor Jurídico. Disponível em:https://www.conjur.com.br/2021-mar-31/garantias-consumo-problema-consentimento-inf ormado-lgpd/. Acesso em 04 de junho de 2025.

Tepedino, Gustavo. Teffé, Chiara Spadaccini de. O consentimento na circulação dos dados pessoais. Revista Brasileira de Direito Civil - RBDCivil. Belo Horizonte.Volume 25. 2020.

BRASIL. Projeto de Lei nº 36/2025. Altera a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados – LGPD), para proibir a oferta mediante pagamento de disponibilidade de dados biométricos sensíveis e estabelecer medidas mais rigorosas de proteção a esses dados. Disponível em https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2482180. Acesso em 06 de junho de 2025.