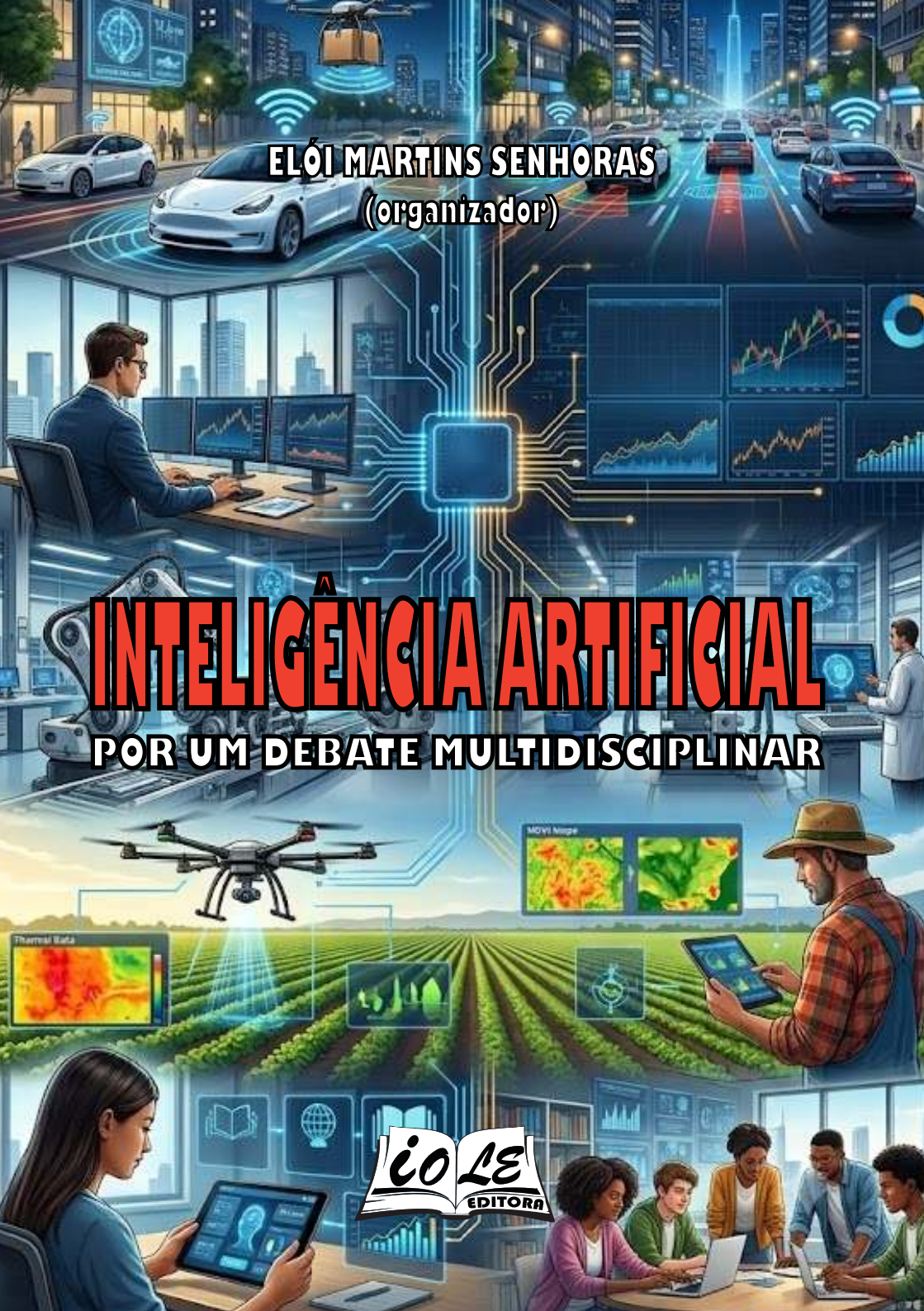
ELÓI MARTINS SENHORAS
(organizador)

INTELIGÊNCIA ARTIFICIAL

POR UM DEBATE MULTIDISCIPLINAR



IOLE EDITORA

INTELIGÊNCIA ARTIFICIAL

Por um Debate Multidisciplinar

INTELIGÊNCIA ARTIFICIAL

Por um Debate Multidisciplinar

ELÓI MARTINS SENHORAS
(organizador)

BOA VISTA/RR
2026

Editora IOLE

Todos os direitos reservados.
A reprodução não autorizada desta publicação, no todo ou em parte, constitui violação dos direitos autorais (Lei n. 9.610/98) é crime estabelecido pelo artigo 184 do Código Penal.



EXPEDIENTE

Revisão
Elói Martins Senhoras
Geane Ribeiro Silva Monteiro

Capa
Alokike Gael Chloe Hounkonnou
Elói Martins Senhoras

Projeto Gráfico e Diagramação
Elói Martins Senhoras
Balbina Líbia de Souza Santos

Conselho Editorial
Abigail Pascoal dos Santos
Charles Pennaforte
Claudete de Castro Silva Vitte
Elói Martins Senhoras
Fabiano de Araújo Moreira
Julio Burdman
Marcos Antônio Fávaro Martins
Rozane Pereira Ignácio
Patrícia Nasser de Carvalho
Simone Rodrigues Batista Mendes
Vitor Stuart Gabriel de Pieri

DADOS INTERNACIONAIS DE CATALOGAÇÃO-NA-PUBLICAÇÃO (CIP)

Se74 SENHORAS, Elói Martins (organizador).

Inteligência Artificial: Por um Debate Multidisciplinar. Boa Vista: Editora IOLE, 2026.

Série: Ciências Sociais. Editor: Elói Martins Senhoras.

ISBN: 978-65-977111-0-9

1 - Empiria. 2 - Estudos de Caso. 3 - Inteligência Artificial. 4 - Multidisciplinaridade. 5 - Teoria.
I - Título. II - Senhoras, Elói Martins. III - Ciências Sociais. IV - Série

CDD–300

A exatidão das informações, conceitos e opiniões é de exclusiva responsabilidade dos autores.
O presente livro contou com avaliação às cegas no sistema double-blind-review.



EDITORIAL

A editora IOLE tem o objetivo de divulgar a produção de trabalhos intelectuais que tenham qualidade e relevância social, científica ou didática em distintas áreas do conhecimento e direcionadas para um amplo público de leitores com diferentes interesses.

As publicações da editora IOLE têm o intuito de trazer contribuições para o avanço da reflexão e das práxis em diferentes áreas do pensamento e para a consolidação de uma comunidade de autores comprometida com a pluralidade do pensamento e com uma crescente institucionalização dos debates.

O conteúdo produzido e divulgado neste livro é de inteira responsabilidade dos autores em termos de forma, correção e confiabilidade, não representando discurso oficial da editora IOLE, a qual é responsável exclusivamente pela editoração, publicação e divulgação da obra.

Concebido para ser um material com alta capilarização para seu potencial público leitor, o presente livro da editora IOLE é publicado nos formatos impresso e eletrônico a fim de propiciar a democratização do conhecimento por meio do livre acesso e divulgação das obras.

Prof. Dr. Elói Martins Senhoras

(Editor Chefe)

Copyright © Editora IOLE
2026

CAPÍTULO 6

Inteligência Artificial: Escore de Crédito, Tratamento e Proteção de Dados Pessoais

INTELIGÊNCIA ARTIFICIAL: ESCORE DE CRÉDITO, TRATAMENTO E PROTEÇÃO DE DADOS PESSOAIS

Luiz Otávio Pimentel[1]

Fabiana Bitencourt[2]

Priscila Peppe[3]

A temática do crédito, sua estrutura conceitual e seus desdobramentos tecnológicos e jurídicos representa, na contemporaneidade, um dos pilares centrais do sistema financeiro global. Muito mais do que uma ferramenta de viabilidade econômica, o crédito é expressão de confiança, relação social e construção de reputação. Neste artigo, observa-se uma abordagem multidisciplinar e comparativa que ultrapassa os limites da análise jurídica tradicional e adentra o campo da tecnologia da informação, das políticas públicas, da proteção de dados e da ética digital. A reflexão proposta é profunda: como o escore de crédito se posiciona no mundo atual – marcado por automação, algoritmos e desigualdade informacional?

A análise começa com o conceito amplo de crédito, retomando sua origem etimológica, *creditum*, e reforçando a noção de confiança como essência fundante da operação creditícia. O crédito, em seu núcleo, representa uma aposta no futuro. É a entrega

[1] Professor da Universidade Atitus. Doutor em Direito pela Universidade Nacional de Assunção (UNA). Email para contato: pimentel.lop@gmail.com

[2] Advogada. Mestranda em Direito pela Universidade Atitus. Email para contato: fabiana_acbrasil@hotmail.com

[3] Advogada. Mestranda em Direito pela Universidade Atitus. Email para contato: priscilapeppe.adv@gmail.com

de um valor presente com a expectativa legítima de retorno futuro, operação que transita tanto pelo campo jurídico – com deveres e obrigações – quanto pelo terreno econômico – com riscos, garantias e recompensas. Essa dualidade se revela particularmente relevante à medida que novas tecnologias complexificam as relações entre credores e devedores, tornando os critérios de avaliação mais abstratos, automatizados e, por vezes, inacessíveis ao cidadão comum.

À luz da evolução histórica, o artigo aborda a criação e difusão da pontuação de crédito, destacando a iniciativa pioneira da empresa alemã Schufa como marco na sistematização do perfil de risco de indivíduos. O modelo, inicialmente baseado em práticas comerciais simples – como a observação do comportamento de pagamento de contas de luz – passou a incorporar cálculos estatísticos sofisticados e, mais recentemente, algoritmos de inteligência artificial. A expansão dos dados tratados, as fontes utilizadas (inclusive não financeiras), e a complexidade dos sistemas empregados suscitam inquietações sobre transparência, legitimidade e justiça na tomada de decisão automatizada.

No cenário brasileiro, o texto evidencia a ausência de regulamentação específica sobre escore de crédito, o que contrasta fortemente com o arcabouço legal da União Europeia. A legislação brasileira, embora tenha dispositivos importantes como a Lei geral de proteção de dados pessoais (LGPD) e o Código de defesa do consumidor (CDC), ainda padece pela falta de normativas claras quanto à metodologia de pontuação, à proporcionalidade no uso de dados sensíveis e à garantia de direitos informacionais aos consumidores. A multiplicidade de pontuações entre diferentes instituições e a utilização obscura de dados criam um terreno fértil para conflitos judiciais, como atestam as milhares de ações e os temas repetitivos julgados pelo Superior Tribunal de Justiça (STJ).

A inteligência artificial (IA) é apresentada como uma virada de chave nesse contexto, ao substituir sistemas baseados em regras administrativas das empresas por modelos preditivos. O aprendizado de máquina e o processamento de linguagem natural permitem avaliações mais dinâmicas, que capturam nuances comportamentais e exploram dados alternativos, como hábitos de consumo, padrões de mobilidade e até interações em redes sociais. Apesar disso, o uso de IA traz riscos relevantes: vieses algorítmicos, ausência de explicação compreensível ao titular dos dados, exposição indevida de informações e vulnerabilidades de segurança, como revela o caso XP de vazamento de dados no Brasil.

Com base em estudos de caso e jurisprudências da Alemanha, Suécia e Áustria, o artigo demonstra como diferentes jurisdições tratam o conflito entre segredo comercial e direito de acesso à informação. A interpretação do Regulamento geral sobre a proteção de dados (RGPD) pelo Tribunal de Justiça da União Europeia (TJUE) vem se consolidando no sentido de garantir aos indivíduos não apenas o conhecimento sobre o uso de seus dados, mas também o direito de não serem afetados por decisões automatizadas sem a devida justificativa. O direito à explicação, antes visto como sugestivo, ganha *status* normativo, impondo às empresas a responsabilidade de oferecer informações inteligíveis sobre os critérios que influenciaram decisões de crédito.

A proposta do artigo é clara e ambiciosa: fomentar a reflexão crítica sobre o uso da IA na pontuação de crédito, identificando os desafios legais, éticos e sociais envolvidos. Ao alinhar conceitos clássicos com análises contemporâneas, o estudo propõe uma jornada rumo à construção de um sistema de crédito mais justo, transparente e inclusivo, que respeite os direitos dos consumidores sem comprometer a inovação financeira. É nesse contexto que se desenrola uma narrativa marcada por contrastes: entre avanço

tecnológico e proteção de dados; entre segredo empresarial e direito à explicação; entre eficiência algorítmica e justiça social.

Para balizar o estudo foi fundamental contar com a revisão bibliográfica abrangente de modelos e análise preditiva de IA em pontuação de crédito realizada por Addy *et al.* (2024)

Cabe registrar que parte deste estudo foi apresentado no II° Seminário Ítalo-Brasileiro Unipg-Atitus, "Direito, Democracia e Tecnologia", em Perúgia (Itália), e parte apresentada e publicada, pelos coautores Pimentel, Raszl Pimentel no Encontro Internacional do Conpedi – "Direito 3D Law", realizado no Instituto Politécnico do Cávado e Ave, Barcelos (Portugal).

O CRÉDITO E A PONTUAÇÃO DE CRÉDITO

O conceito amplo de crédito

O vocábulo crédito significa confiança. Conforme De Plácido e Silva (2014), crédito deriva do latim *creditum*, que possui uma ampla significação econômica e um estreito sentido jurídico:

> Em sua acepção econômica significa a confiança que uma pessoa deposita em outra, a quem estrega coisa sua, para que, em futuro, receba dela coisa equivalente. A confiança gozada por uma pessoa no ânimo daquela de quem se vai tornar devedora, em virtude da entrega atual de coisa, que vai ser transformada em prestação futura, fundamenta o próprio conceito de crédito, em seu aspecto econômico. E esta confiança, indicativa do crédito, generaliza-se a todas as relações comerciais, tomando as mais variadas formas de câmbio de coisas atuais e

> presentes contra coisas equivalentes no futuro, servindo de base a uma série avantajada de operações mercantis. Charles Gide o considera como um alargamento da troca, definindo-o como "a troca de uma riqueza presente por uma riqueza futura". Mas, em realidade, nesse sentido, já vemos o crédito na sua função econômica, sem fugir ao sentido de confiança da pessoa, que dá a coisa presente, na solvabilidade da pessoa que se obriga a entregar a coisa futura. O crédito se constitui, na realidade comercial, sob as modalidades de vendas a prazo ou de empréstimos. E, nesta razão, distinguem-se como elementos componentes: a) a entrega da coisa vendida ou emprestada para ser consumida pelo devedor; b) a espera, pelo credor, da coisa nova que vem substituir a coisa vendida ou emprestada.
>
> Crédito. Juridicamente, significa o direito que tem a pessoa de exigir de outra o cumprimento da obrigação contraída. Neste sentido, no entanto, tem-se o vocábulo em acepção mais ampliada, pois que abrange as obrigações de dar, fazer ou não fazer. Mas, em Direito, ainda possui sentido mais restrito, desde que pode indicar o direito de cobrar uma dívida ativa, como pode significar o próprio título dessa dívida. E, assim, se entende por que tais títulos, em verdade, representam o próprio valor da obrigação a exigir, mostrando-se, por isso, o instrumento do próprio crédito ou o título do crédito.

A operação de crédito, num negócio jurídico de financiamento de pessoa física, tem um sujeito chamada "credor", geralmente uma instituição financeira que empresta uma certa quantia a outra pessoa, chamada "devedor" ou "mutuário", que então garante ao credor que devolverá esse montante financiado dentro do prazo previamente estipulado, mais um valor adicional popularmente chamado "juro". Assim, é uma ferramenta financeira

que permite que pessoas físicas acessem fundos para fazer investimentos, compras, obter serviços, quitar dívidas ou apenas obter dinheiro, sem precisar pagar o montante total de uma só vez no ato do negócio – à vista.

Como se vê no dicionário de Sandroni (1999), o crédito inclui duas noções fundamentais: a "confiança", expressa na promessa de pagamento, e o "tempo" entre o ato da contratação e a liquidação da dívida. Em muitos casos, os próprios vendedores financiam o cliente, todavia, em escala cada vez maior, são as financeiras especializadas que pagam o vendedor e adquirem a dívida sub-rogando-se nos direitos e assumindo o risco de não-pagamento. O lucro da financeira é formado pelos serviços cobrados do devedor. Os cartões de crédito são uma forma de crédito direto ao consumidor.

O financiamento de casas e apartamentos constitui o chamado crédito imobiliário, que envolve pouco risco, pois em geral o próprio imóvel é a garantia do empréstimo, sob a forma de hipoteca. Mas o crédito garantido não foi objeto deste estudo.

A pontuação de crédito

Trazemos a seguir, como exemplo para facilitar a compreensão do tema, a empresa Schufa da Alemanha.

A ideia de instituir a Schufa teve origem no ano 1927, vinda de um funcionário da *Berliner Elektrizitätswerke*, empresa de eletrecidade de Berlim, baseada na prática dos cobradores de eletricidade que tinham uma visão geral de quem pagava as contas de eletricidade regular e pontualmente e de quem era inadimplente, ele teve a ideia de vender aparelhos elétricos, como geladeiras, para os "bons pagadores" em parcelas. Ele sabia, com base nessa

observação, que os beneficiários do crédito cumpririam com suas obrigações de pagamento (SCHUFA, 2025).

A prática de realizar negócios de crédito com base no histórico de pagamentos atraiu o interesse de empresas, especialmente para contar com os serviços especializados de verificação de perfil de bons pagadores. Assim, foi fundada a *Schutzgemeinschaft für allgemeine Kreditsicherung* (Schufa), autocaracterizada como uma comunidade de proteção para garantia geral de crédito, por meio da qual as empresas interessadas podem relatar e consultar informações sobre o comportamento de pagamento de seus clientes (SCHUFA, 2025).

A Schufa, segundo apregoado por ela, ajuda as pessoas a cumprirem seus desejos financeiros de forma simples, rápida e segura. Trabalha para garantir que as pessoas possam fazer negócios de forma conveniente e rápida e que as empresas confiem nelas – sem conhecê-las pessoalmente. Ao fazê-lo, reduz os riscos de inadimplência para provedores de empréstimos, bens e serviços, o que possibilita mais negócios em boas condições, promovendo assim o crescimento e a prosperidade na Alemanha (SCHUFA, 2025).

As soluções da Schufa, segundo apregoado por ela, constantemente aperfeiçoadas, acompanham os negócios comerciais desde a identificação e cálculo do crédito até a prevenção de fraudes e conformidade regulatória. Contribuindo para a prevenção da lavagem de capitais e ajudando a limitar os danos econômicos resultantes da utilização do crédito (SCHUFA, 2025).

Como se vê anunciado no site da empresa:

> Número de pessoas com dados armazenados: 69 milhões;
>
> Número de empresas com dados armazenados: 6,5 milhões;

> Número de clientes corporativos: aproximadamente 11.000;
>
> Informações de acompanhamento para clientes corporativos: 221,3 milhões;
>
> Número de clientes particulares: 2,3 milhões;
>
> Informações para consumidores: 4 milhões;
>
> Receita: € 285.316.000;
>
> Funcionários: mais de 1.000;
>
> Sede em Wiesbaden [capital do estado de Hesse], estabelecimentos regionais em Berlim, Bochum, Hamburgo, Hanover, Colônia e Munique, escritórios em todo o país (SCHUFA, 2025).

Considerando que a população da Alemanha é estimada em 84 milhões de habitantes, os indicadores acima dos dados armazenados pela Schufa são impressionantes.

RGPD: definições

O RGPD estabelece regras gerais para proteger as pessoas singulares no que diz respeito ao tratamento de dados pessoais e para assegurar a livre circulação de dados pessoais na União, é um dos principais marcos legislativos da UE, que permitiu a harmonização em matéria de direito da proteção de dados nos Estados-Membros. No art. 4, constam as seguintes definições operacionalizadas neste estudo:

> 1) “Dados pessoais”, informação relativa a uma pessoa singular identificada ou identificável («titular dos

dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

2) "Tratamento", uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição;

3) "Definição de perfis", qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações.»

4) "Pseudonimização", o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável;

> 5) “Ficheiro” [banco de dados], qualquer conjunto estruturado de dados pessoais, acessível segundo critérios específicos, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico [...].

Na UE a proteção das pessoas singulares, no que diz respeito ao tratamento de dados pessoais, é um direito fundamental (art. 8, nº 1, da Carta dos Direitos Fundamentais da UE; art. 16, nº 1, do Tratado sobre o Funcionamento da UE, art. 8 da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais) – todas as pessoas têm direito à proteção dos seus dados de caráter pessoal que lhes digam respeito.

Brasil: escore de crédito e linhas gerais da regulação

No Brasil, o escore de crédito começou a ser utilizado entre o final do Século XX e início do Século XXI. Sua utilização informatizada como a conhecemos hoje iniciou em 2017 através do Serasa Experian (2025).

Conforme informações extraídas do Banco Central do Brasil (jun. 2025), os gestores de bancos de dados autorizados a prestar serviços de escore de crédito no País são: (i) Boa Vista Serviços S.A., nome fantasia Quod; (ii) Gestora de Inteligência de Crédito S.A.: (iii) SERASA S.A., (iv) Serviços para o Comercio do Brasil S.A.; e (v) Transunion Brasil Sistemas em Informática LTDA (BRASIL, 2025).

No Brasil ainda não existe um marco regulatório específico para o escore de crédito, como existe na UE, não há regras acerca do método de cálculo, nem critérios na elaboração da fórmula

algorítmica e nem mesmo sobre o peso que cada informação pode ou deva representar sobre o escore do consumidor.

As normas mais próximas, que podem ser aplicáveis aos conflitos envolvendo o escore de crédito no Brasil, em ordem cronológica, são: Lei nº 8.078, de 1990, Código de defesa do consumidor; Lei nº 12.414, de 2011; Lei nº 12.965, de 2014; Lei 13.709, de 2018, Lei Geral de Proteção de Dados Pessoais; e as normas da Autoridade Nacional de Proteção de Dados, órgão criado pela Lei nº 13.853, de 2019. A LGPD, em linhas gerias, estabelece regras sobre a obtenção, utilização, proteção e compartilhamento de dados e da formação do histórico de crédito do consumidor.

O serviço de escore de crédito praticado pelas empresas especializadas, por sua vez, se consolida de maneira obscura para o consumidor, uma vez que a falta de um marco regulatório específico possibilita aos gestores de banco de dados desenvolverem seus próprios métodos de cálculo, o que se evidencia pela diferença de pontuação obtida pelo mesmo indivíduo numa ou noutra empresa de escore.

No que tange a transparência, os prestadores de serviço de escore, justificam o sigilo como uma necessidade para a proteção do segredo empresarial (comercial e industrial), ao amparo do art. 19, §3º da LGPD.

No entendimento de Gonçalves (2022), a LGPD permite dúbia interpretação, posto que "o direito de acesso, de transparência, de informação, e a possibilidade de mitigação ficam prejudicados, já que as organizações podem se utilizar desse argumento para negar direito ao consumidor", o segredo empresarial é um salvo conduto para que essas empresas possam manipular os dados pessoais do consumidor.

O avanço tecnológico, por sua vez, associado ao uso cada vez mais intenso do escore de crédito pelas instituições financeiras,

resultou em uma quantidade expressiva de negativas de crédito que, aliadas à opacidade na métrica avaliativa e no modo de utilização dos dados, ensejou um número significativo de ações indenizatórias e o questionamento da licitude do método.

Segundo se vê do voto do Ministro Paulo de Tarso Sanseverino, sobre o desrespeito aos limites legais na utilização do sistema de escore de crédito, configurando abuso no exercício desse direito, que pode ensejar a ocorrência de danos morais nas hipóteses de utilização de informações excessivas ou sensíveis, bem como nos casos de recusa indevida de crédito pelo uso de dados incorretos ou desatualizados, citou que no Tribunal de Justiça do Estado do Rio Grande do Sul, as demandas dessa natureza haviam atingido a expressiva quantidade de cerca de oitenta mil ações, caracterizando o que o anterior código de processo civil, no Art. 543-C, denominava de "multiplicidade de recursos" (BRASIL, 2014).

No Brasil, desde 2018, o Conselho Monetário Nacional, determina que as instituições financeiras autorizadas as funcionar devem implementar e manter política de segurança cibernética formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados, com vistas a preservar os dados e informações sob sua responsabilidade (BRASIL, 2018).

Determina ainda o Conselho Monetário brasileiro, que caberá as instituições financeiras autorizadas ter procedimentos e adotar controles para reduzir a vulnerabilidade da instituição a incidentes; deter os controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis; realizar o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição; as diretrizes para a elaboração de cenários de incidentes considerados nos testes de continuidade de

negócios; e as iniciativas para compartilhamento de informações sobre os incidentes relevantes (BRASIL, 2021).

Assim como, em se tratando de serviços de terceiros, deverá ter a definição de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da instituição; a classificação dos dados e das informações quanto à relevância; e a definição dos parâmetros a serem utilizados na avaliação da relevância dos incidentes (BRASIL, Resolução CMN nº 4.893, de 2021).

Tudo isso garantindo que a instituição financeira autorizada tenha capacidade para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético e consequente proteção da integridade, da disponibilidade dos dados e dos sistemas de informação utilizados (BRASIL, 2021).

Determina ainda, a referida resolução, que é autorizado que as instituições financeiras terceirizem os serviços, mas desde que sejam asseguradas em suas políticas, estratégias e estruturas a observância ao devido gerenciamento de riscos, e se os serviços contratados junto a terceiros sejam relevantes no processamento e armazenamento de dados e de computação em nuvem, no País ou no exterior; a instituição contratante deve considerar a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado (BRASIL, 2021).

Neste sentido as instituições devem previamente à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, adotar procedimentos que contemplem o que está disposto no art. 12 da Resolução CMN nº 4.893, de 2021.

A instituição contratante dos serviços de terceiros será a responsável pela confiabilidade, integridade, disponibilidade, segurança, sigilo em relação aos serviços contratados e ao cumprimento das normas em vigor no Brasil.

Além da comunicação prevista pela LGPD, a instituição financeira deverá realizar junto ao Banco Central do Brasil, a comunicação tempestiva das ocorrências de incidentes relevantes e das interrupções dos serviços relevantes prestados por ela e que configurem uma situação de crise pela instituição financeira, bem como das providências para o reinício das suas atividades, quando for o caso.

A Resolução BCB nº 342, de 2023, do Banco Central do Brasil, determina que as instituições participantes de arranjo de pagamentos Pix, devem comunicar aos titulares de contas de pessoas físicas a ocorrência de incidente de segurança com dados pessoais envolvendo banco de dados, mesmo que a instituição financeira participante não seja a responsável direta pelo incidente e ainda que o incidente de segurança não acarrete risco ou dano relevante aos titulares, ou seja, independente do dano a comunicação deverá ser realizada, ou seja, o titular dos dados deve ser cientificado.

ESCORE DE CRÉDITO NÃO GARANTIDO E A INTELIGÊNCIA ARTIFICIAL

A pontuação de crédito não garantido é um pressuposto fundamental do acesso de uma pessoa ao crédito.

Nos Estados Unidos, por exemplo, existem as agências de crédito e as agências de classificação de crédito que cumprem essa função de acesso para os mutuários. Agências semelhantes existem em muitos outros países. As pontuações de crédito afetam a

concessão e os termos do empréstimo, variando com a utilização e os reembolsos ou não dos créditos (CHATTERJEE *et al.,* 2023).

As "agências de crédito" coletam dados e os transformam em informações sobre consumidores individuais, que são compiladas em relatórios de crédito e comercializados. Essas informações são usadas para criar pontuações de crédito para indivíduos (INVESTOPEDIA, 2025).

As "agências de classificação de crédito" avaliam a força financeira dos emissores de dívida, como grandes empresas, e de suas ofertas de dívidas individuais, para o benefício de investidores e outros interessados. Os emissores lançam no mercado títulos de dívida para captar recursos financeiros. As classificações são normalmente encomendadas e pagas pelos próprios emissores. A classificação de crédito de uma empresa tem relevância na avaliação de investimentos ou da contratação de seguro de uma empresa. As três principais agências internacionais de classificação de crédito são a *Fitch Ratings, Moody's Corporation e S&P Global*. As classificações são baseadas em informações sobre as finanças da empresa, seu setor, os mercados em que ela opera e outros fatores. O objetivo final é avaliar a probabilidade de que um tomador de crédito possa pagar suas dívidas. A *S&P Global* caracteriza as classificações de crédito como "opiniões com visão de futuro sobre a capacidade de crédito relativa de um emissor" (INVESTOPEDIA, 2025).

A função da pontuação de crédito no mercado de crédito é, em parte, avaliar o tipo não observável de uma pessoa. A reputação de uma pessoa é formada por informações ocultas sobre uma característica individual persistente e relevante para o crédito – ser potencialmente um bom pagador. A teoria do comportamento no crédito não garantido e de pontuações de crédito leva em conta alocações e arranjos, sendo que o incentivo para manter uma boa reputação desempenha um papel central, moldando o

comportamento frente ao empréstimo e a poupança ao longo da vida dos indivíduos (CHATTERJEE *et al.,* 2023).

Os dados pessoais básico coletados pelas instituições financeiras e no comércio em geral para cadastro dos clientes são: nome, data nascimento, filiação, endereço, telefone, e-mail, documento de identidade e CPF, rendimentos e número de dependentes, podendo incluir foto (WISE, 2025). Dados pessoais sensíveis também poderão ser coletados, como a origem racial ou étnica, estado de saúde e biometria. Após a abertura de uma conta, os depósitos e os negócios realizadas geram os respectivos dados, se houver opção por serviços *online* será habilitado um nome de usuário e uma chave de acesso secreto *password* que são secretos e privativos do titular destes dados.

Sistema de pontuação de crédito

Os sistemas tradicionais de pontuação de crédito eram baseados em regras, com critérios predefinidos para avaliar a capacidade de um indivíduo ou empresa de obter crédito em uma instituição financeira e realizar o pagamento. O sistema atribuía pontos com pesos geralmente fixos a fatores como histórico de utilização de créditos e pagamentos, patrimônio, número de dependentes do indivíduo, a relação entre as dívidas e a renda. Foram eficazes até certo ponto. Os modelos se baseavam na capturar de dados, geralmente fornecidos pelo interessado e as regras careciam de adaptabilidade frente a complexidade dos comportamentos financeiros individuais (ADDY *et al.,* 2024).

Na medida em que as operações de crédito se tornaram massivas, o uso de cartão de crédito é um exemplo, que o compartilhamento e o comércio de dados de clientes proliferaram,

houve a expansão de fontes de dados e a necessidade de integração destes com fontes de dados alternativos. A transição para sistemas orientados por IA representou um afastamento dos modelos com definição rígida de regras para modelos mais flexíveis e responsivos. A evolução das práticas de pontuação de crédito reflete uma jornada de sistemas rígidos baseados em regras para modelos adaptativos tratados por IA, com dinâmica e precisão **(**ADDY *et al.,* 2024).

A IA representa uma mudança de paradigma na pontuação de crédito.

Computar e estabelecer um perfil de crédito de faxineiros, jardineiros, diaristas, condutores de veículos de taxi ou Uber, locadores Airbnb, pedreiros, carpinteiros, empreiteiros e outros prestadores de serviços não empregados, por exemplo, sempre foi um problema ou motivo de exclusão das fontes de crédito.

O acesso a dados alternativos, como informações não financeiras, pagamentos de aluguel, contas de serviços públicos, comportamento na mídia social, incorporam um quadro mais abrangente do hábito e do comportamento financeiros de um indivíduo (BABAWURUN *et al*., 2023).

A integração de dados alternativos permite uma avaliação de risco holística. Indivíduos com histórico de crédito limitado ou excluídos dos modelos tradicionais de pontuação encontraram um caminho para uma avaliação justa. Ao computar-se uma gama diversificada de pontos de dados, os sistemas de pontuação de crédito orientados por IA passaram a oferecer avaliações de risco mais inclusivas e precisas. Os algoritmos de aprendizado de máquina, um subconjunto da IA, oferecem uma abordagem dinâmica e adaptativa **(**ADDY *et al*., 2024).

Algoritmos podem aprender de forma autônoma acessando vastos conjuntos de dados, discernir padrões intrincados e ajustar

pontuações de crédito com base na evolução dos comportamentos financeiros (MAGNUSON, 2020).

Entre as vantagens destaca-se a análise ampla de variáveis, identificação de relações não lineares e de adaptação às mudanças nos cenários financeiros. Modelos de aprendizado de máquina, incluindo regressão, árvores de decisão e redes neurais, permitem uma compreensão diferenciada do risco de crédito individual e previsões com certo grau de precisão do cumprimento de obrigações financeiras de indivíduo (TALAAT *et al*., 2023).

Arquivos de dados de crédito amplos permitem chances de obter avaliações justas e o alcance de metas amplas de inclusão financeira de indivíduos (ÇALLI; COŞKUN, 2021).

A utilização da IA permitiu a proliferação das "fintechs", "financial technology" (tecnologia financeira), termo referente às *startups* ou jovens empresas que desenvolvem produtos financeiros digitais, nas quais o uso da tecnologia é o principal diferencial em relação às empresas tradicionais do setor.

As *fintechs* oferecem diversas soluções, como cartão de crédito, conta digital, cartão de débito, empréstimos, seguros, entre outros, adotando abordagens inovadoras para avaliação de crédito (LESCRAUWAET *et al*., 2022).

Os sistemas de pontuação de crédito com base em IA, ao garantir justiça, transparência e conformidade com os regulamentos de proteção de dados indicam a adoção de considerações importantes. Ao passo que os órgãos reguladores estão ativamente engajados na definição de estruturas para a governança do uso ético e responsável da IA na pontuação de crédito, proporcionando um equilíbrio entre a inovação e a proteção ao consumidor (LESCRAUWAET *et al*., 2022).

Entre os desafios para a pontuação de crédito com base em IA destacam-se: a garantia de precisão e da relevância de dados alternativos, abordagem de possíveis vieses e garantia da privacidade de dados – que são considerações críticas. O equilíbrio entre a inovação e o uso responsável de dados é um imperativo para a integração bem-sucedida de dados alternativos dos tomadores de crédito e para a precisão na avaliação do risco de crédito que interessa para os donos do capital. O que será moldado pela inovação contínua, desenvolvimentos regulatórios e a busca pela inclusão financeira (JONES; HILLER, 2022).

Modelos sofisticados prometem maior precisão preditiva.

Modelos de IA na pontuação de crédito

Os **modelos de regressão** são fundamentais na pontuação de crédito, com o objetivo de estabelecer relações entre variáveis independentes e a variável dependente – o risco de crédito (DUMITRESCU *et al*., 2022).

Os **modelos de regressão linear** preveem pontuações de crédito com base em combinações ponderadas de recursos de entrada. No entanto, variações mais sofisticadas, como **regressão logística**, são comumente empregadas para lidar com resultados binários, por exemplo se um mutuário ficará inadimplente ou não. Esses modelos fornecem uma maneira transparente e interpretável de entender o impacto de diferentes fatores na qualidade de crédito.

As **árvores de decisão** dividem o processo de pontuação de crédito em uma série de nós ou galhos de decisão com base em recursos como renda, dívida pendente e histórico de pagamentos. ***Random Forests*** é uma técnica de conjunto que agrega várias árvores de decisão para aumentar a precisão preditiva, daí a

denominação de floresta. Essa abordagem aborda o sobreajuste (*overfitting*) e melhora a robustez combinando as saídas de várias árvores individuais. As árvores de decisão e florestas aleatórias são eficazes na captura de relacionamentos complexos dentro de conjuntos de dados, proporcionando flexibilidade e precisão na avaliação de risco de crédito (GOLBAYANI; FLORESCU; CHATTERJEE, 2020).

As **redes neurais**, inspiradas na estrutura do cérebro humano, consistem em nós interconectados organizados em camadas. Os recursos de entrada são processados por meio de camadas ocultas, culminando em uma camada de saída que representa a previsão de pontuação de crédito. Esses modelos se destacam ao lidar com padrões intrincados e relacionamentos não lineares nos dados. As redes **neurais *perceptron***[4] **multicamadas** (sigla **MLP**[5]) são comumente empregadas na pontuação de crédito, adaptando seus pesos durante o treinamento do modelo para otimizar a precisão preditiva. O **aprendizado profundo**, um subconjunto do **aprendizado de máquina**, envolve redes neurais com várias camadas que são designadas como redes neurais profundas. Essa arquitetura de programação permite a extração automática de recursos hierárquicos de dados. Na pontuação de crédito, os modelos de aprendizado profundo, particularmente **redes neurais convolucionais**[6] (sigla **CNNs**) e **redes neurais recorrentes** (**RNNs**), aprimoram a compreensão de relacionamentos complexos em diversos conjuntos de dados (GICIĆ; ĐONKO; SUBASI, 2023). O ***deep learning*** se destaca quando confrontado com dados grandes

[4] Modelo de computador ou máquina computadorizada projetada para representar ou simular a capacidade do cérebro de reconhecer e discriminar.

[5] Sigla original de “Multi-layer perceptron”.

[6] Convolucional: refere-se a um código corretor de erro em que determinado grupo de símbolos (com erros comuns) é transformado em outro grupo de símbolos corretos.

e não estruturados, fornecendo uma estrutura robusta para a avaliação de risco de crédito.

Os **modelos de conjunto** combinam as previsões de vários modelos individuais para obter um desempenho superior. **Métodos de aumento**, como *AdaBoost* e *Gradient Boosting*, criam sequencialmente um modelo forte, enfatizando os pontos fracos dos modelos anteriores. O ***Bootstrap Aggregating*** (***Bagging***) e ***Random Forests***, aproveitam o treinamento paralelo de diversos modelos para uma previsão agregada. As técnicas de conjunto aumentam a estabilidade e a precisão dos modelos de pontuação de crédito, reduzindo o risco de sobre ajuste. O **empilhamento de modelos** envolve a combinação de previsões de vários modelos treinando um metamodelo. Essa técnica visa explorar os pontos fortes de modelos individuais enquanto mitiga seus pontos fracos. O empilhamento de diversos algoritmos, como a combinação de regressão, rede neural e modelos de conjunto, aumenta o poder preditivo geral e a robustez do sistema de pontuação de crédito (MUBARAK *et al*., 2023).

A flexibilidade e adaptabilidade desses modelos contribuem para as avaliações de risco de crédito serem mais precisas e diferenciadas.

O método de análise preditiva na pontuação de crédito por IA

A análise preditiva emergiu como uma pedra angular na reformulação das metodologias de pontuação de crédito, oferecendo maior precisão e profundidade na avaliação do risco de crédito (ȚÎRCOVNICU; HAȚEGAN, 2023).

O domínio multifacetado da análise preditiva na pontuação de crédito, tem papel relevante na previsão do risco de crédito por IA sendo explicável e integrando fontes de dados alternativas para

refinar as previsões. A análise preditiva depende de dados históricos para discernir padrões e tendências relevantes para o risco de crédito. Ao analisar os desempenhos de crédito anteriores, os modelos podem identificar os principais fatores que influenciaram a qualidade do crédito. Os sistemas tradicionais de pontuação de crédito geralmente aproveitavam esses dados históricos para fazer previsões com base em padrões estabelecidos **(**ADDY *et al*., 2024). Nesse sentido a ideia que deu origem a Schufa, os bons pagadores das contas de energia elétrica de Berlim poderiam ter crédito para comprar geladeiras e fazer o pagamento parcelado.

A análise preditiva, juntamente com algoritmos de aprendizado de máquina, introduziu uma abordagem dinâmica para pontuação de crédito. Esse modelo se adapta continuamente aos padrões em evolução, permitindo uma previsão responsiva e precisa do risco de crédito. Algoritmos de aprendizado de máquina, incluindo regressão, árvores de decisão e redes neurais, permitem uma compreensão diferenciada de relacionamentos intrincados dentro de conjuntos de dados (ZAKI *et al*., 2024).

A análise preditiva facilita a avaliação de risco em tempo real, afastando-se dos modelos estáticos. Ao incorporar dados atualizados, esses modelos podem ajustar dinamicamente às pontuações de crédito com base nas mudanças de circunstâncias, oferecendo uma representação precisa da credibilidade atual de um indivíduo **(**ADDY *et al*., 2024).

O advento de modelos complexos de IA ressaltou a importância da explicabilidade na pontuação de crédito. A IA explicável, designada como "XAI", se concentra em tornar o processo de tomada de decisão dos modelos de IA transparente e compreensível. Na pontuação de crédito, isso é crucial para garantir a responsabilidade, a conformidade regulatória e a construção de confiança entre consumidores e as instituições financeiras ou de quem concede crédito. A IA explicável desempenha um papel

fundamental na abordagem de questões de viés e justiça na pontuação de crédito (FRITZ-MORGENTHAL; HEIN; PAPENBROCK, 2022).

Ao fornecer insights sobre como os modelos tomam decisões é possível identificar e corrigir vieses (preconceito, propensão, predisposição), garantindo um tratamento justo em diversos grupos demográficos de titulares de dados. Essa transparência promove práticas éticas de pontuação de crédito (ADDY *et al*., 2024).

A IA explicável permite que os consumidores entendam os fatores que influenciam nas suas pontuações de crédito. Essa transparência capacita os indivíduos a tomarem medidas proativas para melhorar sua credibilidade e promover um estado de confiança no processo de pontuação de crédito. A análise preditiva na pontuação de crédito está integrando cada vez mais fontes de dados alternativas além dos dados financeiros tradicionais. Como referido, isso inclui dados não tradicionais, como histórico de pagamento de aluguel, pagamentos de serviços públicos e até mesmo o comportamento nas redes sociais. A incorporação de dados alternativos fornece uma visão mais abrangente dos hábitos financeiros de um indivíduo, especialmente para aqueles que contam com um histórico de crédito limitado.

Fontes de dados alternativos contribuem para avaliações de risco mais robustas, especialmente para indivíduos com arquivos de dados de crédito limitados. Ao considerar uma gama mais ampla de informações, a análise preditiva pode oferecer previsões precisas, reduzindo a dependência das métricas de crédito tradicionais (ADDY *et al*., 2024).

Embora a integração de fontes de dados alternativas apresente oportunidades aos interessados em pontuar o crédito, ela também apresenta desafios, como garantir a privacidade dos dados, abordar possíveis vieses e navegar pela conformidade regulatória.

Equilibrar a inovação com considerações éticas continua sendo crucial para alavancar dados alternativos à análise preditiva na pontuação de crédito.

A análise preditiva tornou-se uma força instrumental na reformulação dos paradigmas de pontuação de crédito. Sua capacidade de prever o risco de crédito, juntamente com a implementação de IA explicável e a integração de dados alternativos, está impulsionando uma abordagem mais sutil, transparente e inclusiva para avaliar a qualidade de crédito. À medida que a tecnologia continua avançando, a análise preditiva provavelmente desempenhará um papel cada vez mais importante na otimização dos modelos de pontuação de crédito para dar precisão sobre a capacidade de pagamento da obrigação, ser justa em relação a pontuação do indivíduo e compreendida pelo consumidor (UZOUGBO; IKEGWU; ADEWUSI, 2023).

Tendências na análise na pontuação de crédito por IA

À medida que a IA remodela o cenário da pontuação de crédito, várias tendências e inovações emergentes redefinem o futuro desse domínio financeiro crítico. A demanda por transparência e interpretabilidade em modelos de IA, por exemplo, vem impulsionando a adoção da IA explicável. O consumidor precisa entender os fatores que influenciam as decisões referentes ao seu crédito. Prevê-se que as técnicas de **XAI**, como modelos de aprendizado de máquina interpretáveis e métodos agnósticos de modelo, ganhem destaque (DWIVEDI *et al*., 2023). Essas abordagens buscam garantir que o processo de tomada de decisão de crédito não seja apenas precisa, mas também compreensível, promovendo a confiança entre os partícipes.

O **processamento de linguagem natural (**sigla PLN, em inglês **PNL**) pode desempenhar um papel fundamental na pontuação de crédito, particularmente na avaliação de fontes de dados não tradicionais. Ao analisar informações textuais não estruturadas, como atividades em redes sociais e avaliações online, a PLN fornece informações valiosas sobre o potencial de um indivíduo para pagar as contas em dia. A integração da PLN aos modelos de pontuação de crédito permite uma compreensão mais abrangente dos tomadores de crédito, aumentando a precisão preditiva. O uso da **tecnologia *blockchain*** está ganhando forças para abordar preocupações como a rastreabilidade e a segurança de dados na pontuação de crédito. A natureza da cadeia de blocos descentralizada e inviolável do *blockchain* garante a integridade e a segurança de informações confidenciais relacionadas ao crédito. Ao fornecer um livro-razão seguro e transparente, o *blockchain* tem o potencial de aumentar a privacidade dos dados, reduzir o risco de fraude e suscitar confiança em credores e tomadores de crédito (DASHOTTAR; SRIVASTAVA, 2021).

Sob a ótica reguladora, a harmonização e o estabelecimento de padrões visam garantir uma abordagem consistente e justa em todo o setor, além de facilitar a circulação dos dados sem violar a privacidade dos seus titulares. Os esforços de harmonização normativa envolvem o estabelecimento de diretrizes claras para o uso responsável da IA abordando questões de não preconceito, não discriminação, definição de práticas éticas na pontuação de crédito e reforço das medidas de proteção ao consumidor. Isso pode fortalecer os regulamentos de privacidade de dados, garantindo a comunicação transparente das decisões de crédito e implementando mecanismos para que os indivíduos entendam as avaliações de crédito orientadas por IA (TANNA; DUNNING, 2023).

Dada a rápida evolução das tecnologias de IA, as estruturas regulatórias devem se manter dinâmicas e adaptáveis. Os órgãos

reguladores podem adotar abordagens ágeis para acompanhar os avanços tecnológicos, incorporando avaliações e atualizações contínuas para enfrentar os desafios emergentes da pontuação de crédito por IA. Essa adaptabilidade é imprescindível para promover a inovação, mantendo a supervisão regulatória. A ascensão das **finanças descentralizadas** (**DeFi**) apresenta uma força disruptiva no cenário de pontuação de crédito. As plataformas DeFi aproveitam as tecnologias *blockchain* e de contratos inteligentes para fornecer crédito e empréstimos descentralizados sem intermediários tradicionais. Os algoritmos de IA podem desempenhar um papel fundamental na avaliação da credibilidade dos tomadores nesses ecossistemas descentralizados, desafiando ainda mais os modelos de pontuação de crédito (KAPLAN; BENLI; ALP, 2023).

Prevê-se que a **internet das coisas** (**IoT**) contribua com dados valiosos para incrementar os modelos de pontuação de crédito. A integração de dados de dispositivos com IoT, como veículos conectados ou sistemas domésticos inteligentes, pode oferecer informações adicionais sobre os comportamentos financeiros e estilos de vida dos indivíduos. Algoritmos de IA que analisam e interpretam esses dados gerados pela IoT podem fornecer uma visão mais holística do risco de crédito. As inovações futuras podem envolver maior colaboração entre empresas de *fintech*, instituições financeiras tradicionais e gigantes da tecnologia. Parcerias entre setores podem levar ao desenvolvimento de modelos abrangentes de pontuação de crédito que aproveitem diversos conjuntos de dados e recursos de IA. Essas colaborações ou parcerias podem impulsionar soluções inovadoras, aumentar a precisão preditiva e ampliar o acesso ao crédito para populações carentes (ALIREZAIE *et al.*, 2024).

O futuro da IA na pontuação de crédito tende a promover ainda mais a convergência de tecnologias emergentes e cenários regulatórios em evolução contínua. À medida que o setor financeiro

se transforma, um equilíbrio entre inovação e salvaguardas regulatórias é imprescindível. A exploração contínua de tecnologias avançadas e a integração cuidadosa da IA nas práticas de pontuação de crédito tendem a tornar os ecossistemas financeiros mais inclusivos, transparentes e confiáveis (RATZAN; RAHMAN, 2024).

Considerações éticas na pontuação de crédito por IA

Embora a IA tenha trazido avanços notáveis para a pontuação de crédito, desafios e limitações devem ser reconhecidos e abordados. IA interpretável, privacidade de dados, preocupações com segurança, o delicado equilíbrio entre precisão e justiça representam áreas críticas que exigem atenção. À medida que o setor financeiro adota a IA na pontuação de crédito, um esforço conjunto para superar esses desafios será fundamental para garantir o uso responsável e ético dessas tecnologias transformadoras (CHIU; LIM, 2020).

A IA inaugurou uma nova era na pontuação de crédito, oferecendo modelos sofisticados que prometem precisão preditiva. No entanto, a integração da IA na pontuação de crédito trouxe à tona considerações éticas e o potencial de viés, levantando preocupações sobre justiça, transparência e conformidade regulatória. Logo, a dimensão ética da pontuação de crédito de IA, requer estratégias para mitigar os vieses, como preconceito, propensão e predisposição na análise de crédito e na pontuação, e de estar adequada ao marco regulatório, a fim de garantir práticas responsáveis de IA (ADDY *et al*., 2024).

Uma das principais preocupações éticas na pontuação de crédito de IA é a falta de transparência e de explicabilidade em modelos complexos. Como os modelos de IA, particularmente as

redes neurais de aprendizado profundo, operam como caixas pretas, entender como eles chegam às decisões de crédito torna-se um desafio. A pontuação de crédito ética exige transparência para estabelecer a confiança entre os tomadores e fornecedores, permitindo que os tomadores compreendam os fatores que influenciam na sua capacidade de crédito. A pontuação ética de crédito de IA requer comunicação clara e consentimento informado. Os consumidores têm o direito de entender as suas informações usadas na avaliação de seu crédito e como os modelos de IA operam no seu caso particular. Promover a transparência e fornecer aos consumidores a capacidade de aceitar ou recusar avaliações orientadas por IA se alinha com as considerações éticas, respeitando os direitos individuais e a privacidade (PETERS *et al*., 2020).

O potencial de resultados discriminatórios em modelos de pontuação de crédito de IA é outra preocupação ética significativa. Proteger os indivíduos da discriminação injusta com base em fatores como raça, gênero ou *status* socioeconômico é fundamental. As práticas éticas de pontuação de crédito enfatizam a necessidade de identificar e corrigir preconceitos para garantir oportunidades iguais para todos os indivíduos que buscam o crédito. Mitigar a predisposição na pontuação de crédito de IA requer medidas proativas. O emprego de técnicas para detecção de desequilíbrio, como no aprendizado de máquina com reconhecimento de justiça, permite a identificação de disparidades nos resultados do modelo. Uma vez identificados vieses de predisposições, ações corretivas podem ser implementadas para garantir avaliações de crédito justas e equitativas para todos os indivíduos (ADDY *et al.,* 2024).

A predisposição geralmente decorre de dados usados para treinar modelos de IA. A pontuação ética de crédito de IA envolve garantir que os conjuntos de dados de treinamento sejam diversos, representativos e livres de predisposições de históricos do indivíduo. Ao incorporar uma ampla gama de dados que refletem com precisão

a diversidade dos solicitantes de crédito, o risco de perpetuar os preconceitos pré-existentes é reduzido. As práticas éticas de pontuação de crédito vão além do desenvolvimento de modelos. O monitoramento e a avaliação regulares de modelos de IA em cenários do mundo real são cruciais. O escrutínio contínuo ajuda a identificar quaisquer predisposições existentes na ampla gama de dados, refletindo com precisão a diversidade dos solicitantes de crédito. O risco de perpetuar os preconceitos pré-existentes é reduzido nas verificações periódicas do modelo, que no caso de dados emergentes ou consequências não intencionais, permite ajustes imediatos para manter a justiça e os padrões éticos (ADDY *et al*., 2024).

A pontuação de crédito ética de IA se alinha com as leis e regulamentos de proteção de dados. A conformidade com estruturas normativas como o RGPD garante que os direitos de privacidade dos indivíduos sejam respeitados. A implementação de práticas robustas de governança de dados e a obtenção de consentimento explícito para o uso de dados contribuem para a conformidade ética. Os órgãos reguladores desempenham um papel fundamental na garantia de práticas éticas de pontuação de crédito de IA. Aperfeiçoar as diretrizes, padrões e mecanismos de supervisão para serem claros ajuda a responsabilizar as instituições por processos ilegais de avaliação de crédito orientados por IA. As considerações éticas são integradas nos quadros regulamentares para salvaguardar os direitos dos consumidores e prevenir práticas discriminatórias **(**ADDY *et al*., 2024).

A pontuação de crédito ética envolve a implementação de estruturas de governança de IA responsáveis dentro das organizações. Isso inclui a existência ativa de comitês de ética de IA, a realização de avaliações de impacto e a promoção de uma cultura de uso responsável da IA. O alinhamento com os princípios éticos de IA reconhecidos pelo setor garante um compromisso com os padrões éticos nas práticas de pontuação de crédito.

A inclusão de considerações éticas e mitigar o viés nas predisposições de pontuação de crédito de IA é essencial para promover confiança, justiça e responsabilidade. A transparência, o consentimento informado e a proteção contra discriminação são princípios éticos fundamentais.

Ao empregar técnicas para detectar e corrigir predisposições, garante-se que os conjuntos de dados diversificados e representativos do indivíduo se alinhem com as estruturas regulatórias, assim, sem dúvida, o setor financeiro ganha e mantém a credibilidade ao adotar práticas éticas de pontuação de crédito de IA (LAINEZ; GARDNER, 2023).

O monitoramento contínuo, a avaliação e a governança responsável da IA contribuem ainda mais para a construção de um cenário de pontuação de crédito tecnologicamente avançado e eticamente robusto. À medida que o setor continua a navegar na interseção de IA e pontuação de crédito, o compromisso com práticas éticas continuará sendo essencial para a construção de um ecossistema financeiro confiável e inclusivo (ADDY *et al*., 2024).

Como se vê, o uso da IA levanta diversas questões éticas complexas que precisam ser consideradas. A possibilidade de vieses algorítmicos, responsabilização, segurança e abertura são as principais preocupações éticas em torno da IA nas finanças. A IA em processos de tomada de decisão, como avaliação de risco e aprovação de empréstimos, levanta questões sobre explicabilidade, justiça e a possibilidade de discriminar resultados, inclusive na divisão entre países avançados e os menos desenvolvidos. O estabelecimento de procedimentos de reclamação por tratamento injusto em sistemas de IA e a promoção da transparência para os consumidores sobre a tomada de decisões algorítmicas são todos necessários para lidar com vieses e garantir a justiça na IA. Será o ideal a criação de sistemas de IA imparciais que sejam transparentes, equitativos e confiáveis (SETH, 2024).

Wulf e Seizov (2024) fizeram uma revisão da jurisprudência recente sobre o acesso de titulares de informações sobre os algoritmos que os afetaram. Verificaram que o Tribunal Distrital de Amsterdã concedeu acesso judicial às informações de titulares de dados em um para cada três casos de pedidos recebidos. Os titulares dos dados tiveram que demonstrar ao tribunal que seus direitos foram significativamente afetados negativamente por um escore totalmente automatizado que processou seus dados e negou crédito sem a intervenção humana. O titular dos dados em um dos casos era motoristas de táxi, filiado e possivelmente apoiado por um sindicato. Parece improvável que os titulares dos dados na qualidade de consumidores possam e estejam regularmente aptos a ter acesso aos algoritmos que os afetam. No processo de um dos casos que chegou ao tribunal, as pessoas que promoveram a demanda descobriram que o processo decisório de que se queixavam não era totalmente automatizado. Outro caso, envolvendo a Uber como controladora de dados, demonstrou que a supervisão humana estava de fato envolvida na decisão negativa ao consumidor e o pedido de acesso às informações sobre o algoritmo empregado foi negado. Os resultados dessa revisão jurisprudencial demonstraram como podem ser imprecisas e não transparentes as informações que as empresas fornecem aos consumidores sobre o uso de algoritmos de IA.

Segundo Wulf e Seizov (2024), seria muito otimista esperar que a jurisprudência nova e abrangente surja em breve e que mude fundamentalmente o *status quo* atual. Sustentam que, no passado, os tribunais alemães não se tornaram famosos pelo contributo para promover a transparência das divulgações aos consumidores. Por outro lado, evidências sugerem que as empresas estão atualmente cautelosas e temem que os tribunais permitam acesso às informações aos consumidores afetados se forem submetidas a recurso judicial nas instâncias superiores. De acordo com a estrutura legal atual, é razoável esperar que as empresas implementem as sugestões de melhoria como adições não vinculativas às suas políticas de

privacidade e termos e condições, por exemplo, na forma de perguntas frequentes, vídeos explicativos ou fontes de esclarecimentos similares. Resta esperar que o aumento da conscientização pública e a priorização atual dos formuladores de políticas sobre a ética, o controle e a supervisão da IA motivem as autoridades de proteção de dados e as organizações de consumidores a monitorar melhor e possivelmente evocar a conformidade do mercado, apoiando assim os apelos por uma melhor transparência da IA. Na opinião dos autores, certamente há trabalho a ser feito: o Facebook, por exemplo, a maior rede social do mundo, nunca se preocupou em responder às solicitações de informações sobre o uso de algoritmos de IA ignorando assim suas obrigações sob o RGPD.

ESTUDO DE CASOS

Brasil

Tema 710 e Súmula 550 do STJ

Para colocar fim às discussões sobre o escore de crédito e pacificar a jurisprudência, em 2014 o STJ (REsp 1.419.697/RS) publicou a decisão, com o Tema Repetitivo 710 (Tema 710), onde ficou firmada a seguinte tese:

> I. O sistema "credit scoring" é um método desenvolvido para avaliação do risco de concessão de crédito, a partir de modelos estatísticos, considerando diversas variáveis, com atribuição de uma pontuação ao consumidor avaliado (nota do risco de crédito);

II. Essa prática comercial é lícita, estando autorizada pelo art. 5º, IV, e pelo art. 7º, I, da Lei n. 12.414/2011 (lei do cadastro positivo);

III. Na avaliação do risco de crédito, devem ser respeitados os limites estabelecidos pelo sistema de proteção do consumidor no sentido da tutela da privacidade e da máxima transparência nas relações negociais, conforme previsão do CDC e da Lei n. 12.414/2011;

IV. Apesar de desnecessário o consentimento do consumidor consultado, devem ser a ele fornecidos esclarecimentos, caso solicitados, acerca das fontes dos dados considerados (histórico de crédito), bem como as informações pessoais valoradas;

V. O desrespeito aos limites legais na utilização do sistema "credit scoring", configurando abuso no exercício desse direito (art. 187 do CC), pode ensejar a responsabilidade objetiva e solidária do fornecedor do serviço, do responsável pelo banco de dados, da fonte e do consulente (art. 16 da Lei n. 12.414/2011) pela ocorrência de danos morais nas hipóteses de utilização de informações excessivas ou sensíveis (art. 3º, § 3º, I e II, da Lei n. 12.414/2011), bem como nos casos de comprovada recusa indevida de crédito pelo uso de dados incorretos ou desatualizados.

A repercussão sobre o tema foi tamanha, que após a publicação da decisão, o juiz Vilson Fontana, titular da 2ª Vara do Juizado Especial Cível de Florianópolis, Estado de Santa Catarina, editou a Portaria de Julgamento de Processos com Valor Jurídico de Sentença nº 01/2015, e com base nela extinguiu cerca de 55 mil processos que tinham como causa dos litígios o sistema de escore de crédito naquele juizado.

Posteriormente ao julgamento do Tema 710 no STJ, objetivo uniformizar a interpretação da lei federal e orientar a comunidade

jurídica, sintetiza a jurisprudência predominante no tribunal, foi instituída a Súmula 550 (REsp 1.419.697 e REsp 1.457.199), publicada em 19/10/2015, proclamando que o escore de crédito não é um banco de dados e, portanto, dispensa a necessidade de prévio consentimento do consumidor tanto para cálculo da pontuação quanto para sua utilização, nos seguintes termos:

> A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo.

No que tange o direito à informação, tanto o Tema 710 quanto a Súmula 550 ratificaram o direito do consumidor em obter as fontes dos dados considerados para histórico de crédito, bem como as informações pessoais valoradas para aferição do seu escore.

Por fim, ficou estabelecido que ações indenizatórias são possíveis, desde que acompanhadas de prova robusta de que tenha havido negativa de crédito ao consumidor por baixo escore e que esta pontuação tenha sido originada através do uso de dados sensíveis, incorretos ou desatualizados.

Nota-se, contudo, que tais decisões buscam suprir a lacuna normativa sobre o escore de crédito, uma vez que no Brasil, atualmente, os serviços operam de forma lícita com base na jurisprudência sem que haja, para tanto, um marco regulatório sobre o método e a sistemática para sua execução.

Tema 915 do STJ

Diante do novo cenário que se vislumbrou após o Tema 710, de 2014, a opacidade e a obscuridade acerca da fonte, da forma de tratamento e da métrica avaliativa dos dados dos consumidores para cálculo do escore de crédito resultou em um novo contexto, desta vez voltado às demandas cautelares para exibição de documentos em desfavor de entidades de proteção ao crédito, ensejou a edição Tema Repetitivo 915, em 2016.

A **ação cautelar** passou a ser o remédio jurídico dos prejudicados pelo escore de crédito desfavorável, com fundamento nos arts. 844 e 845 e nos arts. 355 a 363 do antigo Código de Processo Civil, de 1973, legislação vigente à época do julgamento do Tema 915, de 2015.

O novo Código de Processo Civil, que entrou passou a vigor em 18/03/2016, mudou o remédio jurídico, as medidas cautelares passaram a ser tratadas dentro da **tutela provisória**, que pode ser antecipada ou cautelar, conforme os artigos 294 a 311 do código de 2016.

Segundo Oliveira (2002), a ação cautelar de exibição tinha por finalidade levantar "o véu, o segredo, da coisa ou do documento, com vistas a assegurar o seu conteúdo e, assim, a prova em futura demanda".

Somente no Tribunal de Justiça do Estado do Rio Grande do Sul, após a publicação do Tema 710, foram mais de três mil ações cautelares exibitórias, em cujo polo passivo figuravam as principais empresas de proteção ao crédito e cuja pretensão deduzida visava a exibição de documentos ou dados concernentes a cadastro ou consultas para concessão de crédito.

Dada a nova multiplicidade de recursos, em 30/03/2016 foi publicada a decisão (REsp 1.304.736/RS) que gerou o Tema 915, definindo os requisitos mínimos para a configuração do direito de agir em ações dessa natureza.

A tese firmada pelo Tema 915 foi a seguinte:

> Em relação ao sistema "credit scoring", o interesse de agir para a propositura da ação cautelar de exibição de documentos exige, no mínimo, a prova de:
>
> i. requerimento para obtenção dos dados ou, ao menos, a tentativa de fazê-lo à instituição responsável pelo sistema de pontuação, com a fixação de prazo razoável para atendimento; e
>
> ii. que a recusa do crédito almejado ocorreu em razão da pontuação que lhe foi atribuída pelo sistema *scoring*.

De acordo com os fundamentos do julgado, a exigência de prévio requerimento foi analisada de forma analógica ao direito previdenciário, onde exige-se prévio indeferimento administrativo para configurar interesse de agir na esfera judicial.

Ao final, o magistrado concluiu que o direito de agir está condicionado à comprovação de que o consumidor tenha previamente requerido informação sobre os dados junto à empresa de escore e que o referido pleito tenha sido recusado ou não atendido em prazo razoável.

Além disso, o consumidor deveria comprovar que tinha sofrido recusa de crédito em razão da pontuação. Ou seja, além da comprovada violação ao previsto na Lei nº 12.414, de 2001, na LGPD e no CDC sobre o direito do consumidor à informação e à transparência sobre o uso e tratamento dos seus dados, o magistrado decidiu por incluir mais uma condicionante no direito de agir em

ação cautelar de exibição de documentos, a comprovada recusa de crédito com base no escore.

Tal situação manifestamente torna onerosa a defesa do direito e dificulta à parte hipossuficiente de recorrer ao judiciário para buscar amparo contra violação de um direito, eis que, como dito, a obtenção da prova, nestes casos, se torna deveras dificultosa ou até mesmo impossível, dada a opacidade que se opera e a ausência de regulamentação específica sobre os métodos aplicados na pontuação de crédito.

Recurso Especial nº 2.133.261/SP e nº 2.115.461/SP: Dano moral in re ipsa pelo compartilhamento de dados não sensíveis a terceiros consulentes que não outros bancos de dados

As recentes decisões judiciais que versam sobre o escore de crédito e os respectivos bancos de dados no Brasil, foram julgadas pela no STJ e publicadas em 10 e 14/10/2024, firmando precedente sobre o tratamento dos dados realizado pelos gestores de banco de dados e a disponibilização a terceiros consulentes que não gestores de banco de dados, sem o prévio consentimento do consumidor, titular dos dados.

Na ação movida em desfavor da Boa Vista Serviços S.A., cuja autora pleiteava obrigação de fazer e danos morais pelo compartilhamento de seus dados não sensíveis a consulentes que não outros gestores de dados, sem prévia autorização e sem consentimento para tal. A autora da ação (consumidor) comprovou que qualquer pessoa pode pagar pelo serviço diretamente no site da ré e extrair, de qualquer CPF, um relatório com dados pessoais, estado civil, endereços, telefones, e-mails, escolaridade, histórico de

créditos além de outras informações, sem que o consumidor fosse informado da venda e da publicidade de seus dados.

A discussão, desse caso, foi levada aos tribunais superiores com a tese sustentada de que a disponibilização de dados pessoais em bancos de fácil acesso por terceiros, sem consentimento do cadastrado (titular dos dados), mesmo que pagos, enseja o direito a indenização por danos morais.

No julgamento, ratificou-se o entendimento de que o escore de crédito dispensa o consentimento do consumidor por não ser considerado um banco de dados, nos moldes do Tema 710 e da Súmula 550 do STJ, que firmou a jurisprudência nestes termos.

Contudo, tal situação não afasta o gestor dos dados da obrigação de cumprir as demais normas que versam sobre o cadastro positivo e o tratamento de dados do consumidor cadastrado, estando, portanto, restrito ao que normatiza o CDC, a LGPD e a Lei do Cadastro Positivo.

De acordo com essa legislação, concluiu o magistrado que a dispensa do consentimento prévio para a abertura do cadastro não significa a dispensa da comunicação e da necessidade de prévio consentimento para disponibilização dos dados coletados a terceiros consulentes. E concluiu que a disponibilização indevida desses dados resulta em ofensa aos limites legais, o que configura o dano moral presumido.

Ao final, julgou procedente os pedidos do autor da ação e condenou a ré na obrigação de fazer para que se abstenha de disponibilizar, de qualquer forma, os dados da autora sem sua prévia autorização, bem como ao pagamento de indenização a título de danos morais, pela violação legal.

Caso XP

No mês de abril de 2025, a XP Investimentos Corretora de Câmbio, Títulos e Valores Mobiliários S/A informou aos clientes, em cumprimento da LGPD, que houve um acesso não autorizado a informações parciais contidas numa base de dados hospedada em um de seus fornecedores externos de serviços:

> Em 22/03/25, tomamos conhecimento de que uma base de dados que se encontrava hospedada em um fornecedor externo da XP teve um acesso não autorizado. Imediatamente efetivamos o bloqueio deste acesso. Sua conta e seus investimentos estão em total segurança, pois nenhum sistema da XP foi acessado. A utilização dos nossos aplicativos e sites pode continuar sendo realizada normalmente e não é necessário alterar sua senha.

Informou ainda quais foram os dados de titularidade dos seus clientes que foram acessados: dados cadastrais, como nome, telefone, e-mail, data de nascimento, CEP, estado civil, gênero, cargo e nacionalidade; dados sobre os produtos financeiros contratados, sem os respectivos detalhamentos, limitando-se às informações binárias, como se possui ou não cartão de crédito e débito, seguro, consórcio, previdência e portabilidade de salário.

Foi reiterado pela XP aos titulares dos dados, que seus recursos estavam em segurança e que dados como o número da conta, saldo, posição, nome do assessor e limite de crédito, referentes ao mês de março; que a conta não foi acessada, nenhuma operação foi feita e que os recursos estavam seguros e protegidos. (XP, e-mail disponível no site <https://cj.estrategia.com/portal/vazamento-dados-xp-responsabilidade-direitos/>.

A XP recomendou aos seus clientes que por conta do ocorrido, realizassem procedimentos de segurança quanto a possíveis ligações telefônicas feitas em nome da XP, para reconhecimento de compras ou transações, ou para que alterassem ou realizem qualquer ação no aplicativo sob orientação de qualquer via telefonia. Foi informado pela XP que ela não solicita dados de senhas, token ou qualquer código recebido por SMS ou e-mail. Se o cliente ficasse em dúvida sobre algum contato suspeito, procurasse os canais oficiais de atendimento da empresa e disponibilizando documento com mais informações de segurança aos clientes.

Os dados indevidamente expostos dos clientes da XP, abrangem diversas categorias, posto que incluíam: dados sensíveis, dados pessoais e financeiros sigilosos. Assim a informação relacionada à pessoa física, identificada ou identificável, é denominada na legislação de dados pessoais, bem como na Lei Complementar nº 105, de 2001, que as instituições financeiras conservem sigilo em suas operações ativas e passivas e serviços prestados.

Conforme art. 6°, incisos I, VI e VII, da LGPD, o tratamento dos dados deverá ser realizado baseado nos princípios da transparência e segurança, de forma previamente livre, informada e inequívoca ao titular dos dados coletados e tratados pela qual ele concorde com o tratamento de seus dados pessoais para uma finalidade determinada, esta que deverá ser segura.

Nesse incidente relevante, pelo disposto no marco regulatório brasileiro, a responsabilidade pelo vazamento de dados é da instituição regulada, no caso a XP, já que esta era a contratante dos serviços terceirizados do armazenamento de sua base de dados violada.

A XP, como relatado, era a controladora dos dados pessoais dos seus clientes e, portanto, responsável nesse incidente,

independente da contratação dos serviços terceirizados, visto que antes ou durante o compartilhamento dos dados deveria ter realizado cabalmente todos os procedimentos de controle e segurança quanto aos dados e informações de seus clientes.

Resta claro que as instituições financeiras devem instituir mecanismos de acompanhamento e de controle rigorosos com vistas a assegurar a implementação e a efetividade da política de segurança cibernética, do plano de ação e de resposta a incidentes e dos requisitos para contratação de serviços de processamento e armazenamento de dados de clientes, mantendo a definição de processos, testes e trilhas de auditoria; a definição de métricas e indicadores adequados; e a identificação e a correção de eventuais deficiências, com vistas a garantir a segurança dos dados de seus clientes.

Logicamente a empresa lesada pela contrata tem direito de exigir o ressarcimento dos prejuízos e exigir o reforço da segurança cibernética. O art. 14 da Resolução CMN n° 4.893, de 2021, dispõe que a instituição contratante dos serviços mencionados no art. 12 é responsável pela confiabilidade, pela integridade, pela disponibilidade, pela segurança e pelo sigilo em relação aos serviços contratados, bem como pelo cumprimento da legislação e da regulamentação em vigor.

O marco regulatório da proteção de dados da LGPD e da Autoridade Nacional de Proteção de Dados brasileira, estabelecem com clareza as responsabilidades e as obrigações dos agentes quanto ao incidente e os direitos dos titulares de dados.

União Europeia

Caso OQ vs. Land Hessen, interveniente SCHUFA Holding AG: "scoring" para tratamento de dados pessoais, Alemanha (TJUE C-634/21, 2023)

Segundo Wulf; Seizov (2024), em um caso histórico em 2014, o Tribunal Federal Alemão decidiu que os algoritmos de *scores* da principal empresa alemã de pontuação de crédito, a Schufa, poderiam permanecer ocultos, confirmando o direito das empresas de manter segredos comerciais. Em 2018, um consumidor exigiu que uma empresa lhe enviasse seu relatório completo de pontuação de crédito, incluindo as pontuações parciais que compunham sua classificação total de crédito, mas o Tribunal Regional de Wiesbaden não considerou sua demanda razoável, esse caso chegou ao TJUE, como será estudado a seguir.

Como se vê do relatório do Juiz Andreas Kumin, o litígio envolve OQ, e o *Land Hessen* (Estado de Hesse na Alemanha), por força da recusa do *Hessischer Beauftragter für Datenschutz und Informationsfreiheit* (HBDI), Comissário para a Proteção de Dados e da Liberdade de Informação do Land de Hesse, de ordenar à Schufa Holding AG (Schufa) que deferisse um pedido apresentado por OQ destinado a aceder e a apagar os dados pessoais que lhe dizem respeito (UNIÃO EUROPEIA, 2023).

A Schufa, como vimos acima, fornece aos seus parceiros contratuais informações sobre a solvabilidade de terceiros, nomeadamente de interessados em obter crédito. Para o efeito, ela estabelece um prognóstico sobre a probabilidade de um comportamento futuro de uma pessoa (escore), como o reembolso de um empréstimo, a partir de certas características dessa pessoa,

tendo por base procedimentos matemáticos e estatísticos utilizando a IA. A determinação dos escores assenta no pressuposto de que a classificação de uma pessoa numa categoria de pessoas com características comparáveis que se comportaram de uma determinada maneira permite prever um comportamento semelhante (UNIÃO EUROPEIA, 2023).

O caso judicializado teve origem na recusa a OQ da concessão de um empréstimo por um terceiro, após a Schufa ter estabelecido e transmitido a esse terceiro informações negativas a seu respeito. OQ pediu à Schufa que lhe desse informações sobre os dados pessoais registados e que apagasse aqueles que pretensamente estavam errados (UNIÃO EUROPEIA, 2023).

Em resposta a esse pedido, a Schufa informou a OQ o nível do seu escore e expôs, genericamente, as modalidades de cálculo dos *scores*. No entanto, se recusou, invocando o segredo comercial, a divulgar as diferentes informações tomadas em conta para os efeitos desse cálculo, bem como a ponderação aplicada. Por último, a Schufa declarou que se limitava a enviar as informações aos seus parceiros contratuais e que eram estes últimos que tomavam as decisões contratuais propriamente ditas de dar ou não um crédito (UNIÃO EUROPEIA, 2023).

Mediante a reclamação apresentada em 18/10/2018, OQ pediu ao HBDI, autoridade de proteção de dados e da liberdade de informação competente, que ordenasse à Schufa que deferisse o seu pedido de acesso às informações e de apagar os dados errados (UNIÃO EUROPEIA, 2023).

Por decisão de 03/06/2020, o HBDI indeferiu esse pedido, porque não estava demonstrado que a Schufa não teria cumprido os requisitos enunciados no artigo 31 do *Bundesdatenschutzgesetz* (BDSG), lei federal alemã relativa à proteção de dados, que lhe compete no que respeita à sua atividade (UNIÃO EUROPEIA,

2023).

OQ interpôs recurso dessa decisão ao *Verwaltungsgericht Wiesbaden* (Tribunal Administrativo de Wiesbaden, Alemanha), que era o órgão jurisdicional de recurso para o caso em tela. Segundo esse órgão jurisdicional, para decidir o litígio que lhe fora submetido, importava verificar se a determinação de um valor de probabilidade como o que estava em causa no processo principal constituía uma decisão individual automatizada, na acepção do artigo 22, nº 1, do RGPD. Com efeito, em caso afirmativo, a licitude desta atividade estaria subordinada, em conformidade com o artigo 22, nº 2, alínea b), do RGPD, ao requisito de essa decisão ser autorizada pelo direito da UE ou do Estado Membro (Alemanha, no caso) a que o responsável pelo tratamento estivesse sujeito (UNIÃO EUROPEIA, 2023).

O artigo 22 do RGPD dispõe o seguinte:

> **Decisões individuais automatizadas, incluindo definição de perfis**
>
> 1. O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.
>
> 2. O nº. 1 não se aplica se a decisão:
>
> a) For necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento;
>
> b) For autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos

> dados; ou
>
> c) For baseada no consentimento explícito do titular dos dados;
>
> 3. Nos casos a que se referem o nº 2, alíneas a) e c), o responsável pelo tratamento aplica medidas adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados, designadamente o direito de, pelo menos, obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão;
>
> 4. As decisões a que se refere o nº. 2 não se baseiam nas categorias especiais de dados pessoais a que se refere o artigo 9, nº. 1, a não ser que o nº. 2, alínea a) ou g), do mesmo artigo sejam aplicáveis e sejam aplicadas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular.

A esse respeito, o Tribunal Administrativo de Wiesbaden teve dúvidas quanto à tese segundo a qual o artigo 22, nº 1, do RGPD não seria aplicável à atividade de empresas como a Schufa. Fundamentou as suas dúvidas, de um ponto de vista factual, na importância de um valor de probabilidade como o que estava em causa no processo principal para a prática decisória de terceiros aos quais esse valor de probabilidade foi transmitido e, de um ponto de vista jurídico, principalmente nos objetivos prosseguidos pelo artigo 22, nº 1, e nas garantias de proteção jurídica consagradas pelo RGPD. Especificamente, este TJUE destaca que é o valor de probabilidade que normalmente determina se é como o terceiro irá contratar com o titular dos dados. Ora, o artigo 22 do RGPD visa precisamente proteger as pessoas contra os riscos associados às decisões puramente baseadas num automatismo, no caso em algoritmo de IA (UNIÃO EUROPEIA, 2023).

Em contrapartida, se o artigo 22, nº 1, do RGPD devesse ser

interpretado no sentido de que a qualidade de "decisão individual automatizada" só pode ser reconhecida, numa situação como a que estava em causa no processo principal, à decisão tomada pelo terceiro em relação ao titular dos dados, decorreria daí uma lacuna na proteção jurídica. Com efeito, por um lado, uma empresa como a Schufa não está obrigada a dar acesso às informações adicionais a que o titular dos dados tem direito ao abrigo do artigo 15, nº 1, alínea h), do RGPD, uma vez que não é esta empresa que adota uma "decisão automatizada", na acepção desta disposição e, consequentemente, na acepção do artigo 22, nº 1, do RGPD. Por outro lado, o terceiro a quem é comunicado o valor de probabilidade não pode fornecer essas informações adicionais, uma vez que não dispõe das mesmas. Assim, segundo o Tribunal Administrativo de Wiesbaden, para evitar tal lacuna na proteção jurídica, seria necessário que a determinação de um valor de probabilidade como o que está em causa no processo principal esteja abrangida pelo âmbito de aplicação do 22, nº 1, do RGPD (UNIÃO EUROPEIA, 2023).

O artigo 15 do RGPD dispõe o seguinte:

> Direito de acesso do titular dos dados
>
> 1. O titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e às seguintes informações:
>
> a) As finalidades do tratamento dos dados;
>
> b) As categorias dos dados pessoais em questão;
>
> c) Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações

internacionais;

d) Se for possível, o prazo previsto de conservação dos dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo;

e) A existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos dados pessoais no que diz respeito ao titular dos dados, ou do direito de se opor a esse tratamento;

f) O direito de apresentar reclamação a uma autoridade de controlo;

g) Se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem desses dados;

h) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22, nº 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.

2. Quando os dados pessoais forem transferidos para um país terceiro ou uma organização internacional, o titular dos dados tem o direito de ser informado das garantias adequadas, nos termos do artigo 46 relativos à transferência de dados.

3. O responsável pelo tratamento fornece uma cópia dos dados pessoais em fase de tratamento. Para fornecer outras cópias solicitadas pelo titular dos dados, o responsável pelo tratamento pode exigir o pagamento de uma taxa razoável tendo em conta os custos administrativos. Se o titular dos dados apresentar o pedido por meios eletrônicos, e salvo pedido em contrário do titular dos dados, a informação é fornecida num formato eletrônico de uso corrente.

4. O direito de obter uma cópia a que se refere o nº 3 não prejudica os direitos e as liberdades de terceiros.

Se essa interpretação devesse ser acolhida, a licitude dessa atividade dependeria então da existência de uma base jurídica ao nível do Estado Membro em causa, a Alemanha, em conformidade com o artigo 22, nº 2, alínea b), do RGPD. Ora, no caso em apreço, embora o artigo 31 da BDSG possa constituir tal base jurídica na Alemanha, existem dúvidas sérias quanto à compatibilidade desta disposição com o artigo 22 do RGPD, de hierarquia jurídica superior, uma vez que o legislador alemão apenas regulamenta a "utilização" de um valor de probabilidade como o que está em causa no processo principal, e não a determinação enquanto tal desse valor (UNIÃO EUROPEIA, 2023).

Em contrapartida, se a determinação desse valor de probabilidade do escore não constitui uma decisão individual automatizada na acepção do artigo 22 do RGPD, a cláusula de abertura que figura no nº 2, alínea b), do artigo 22 também não se aplica às regulamentações nacionais relativas a essa atividade. Tendo em conta o caráter, em princípio, exaustivo do RGPD e na falta de outra competência normativa para tais regulamentações nacionais, parece que o legislador alemão, ao sujeitar a determinação de valores de probabilidade a requisitos de licitude substantiva mais abrangentes, define a matéria regulamentada indo além das exigências enunciadas nos artigos 6 e 22 do RGPD, sem dispor de poder legislativo para esse efeito. Se este ponto de vista estiver correto, fica alterada a margem de exame da autoridade nacional de controle, a HBDI no caso, que deveria então apreciar a compatibilidade da atividade das sociedades que fornecem informações comerciais à luz do artigo 6 do RGPD (UNIÃO EUROPEIA, 2023).

O artigo 6, nº 1, do RGPD dispõe o seguinte:

Licitude do tratamento [de dados]

1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:

a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;

b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;

c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;

d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;

e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;

f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

O primeiro parágrafo, alínea f), não se aplica ao tratamento de dados efetuado por autoridades públicas na prossecução .

das suas atribuições por via eletrônica.

Nestas condições, o Tribunal Administrativo de Wiesbaden decidiu suspender a instância e submeter ao TJUE as questões prejudiciais.

Foram invocados pelo juiz relator do caso no TJUE os seguintes princípios:

> 67 [...] em conformidade com jurisprudência constante do Tribunal de Justiça, qualquer tratamento de dados pessoais deve, por um lado, ser conforme com os princípios relativos ao tratamento de dados estabelecidos no artigo 5 do RGPD e, por outro, à luz, especialmente, do princípio da licitude do tratamento, previsto no nº 1, alínea a), deste artigo, cumprir um dos requisitos de licitude do tratamento enumerados no artigo 6 deste regulamento (Acórdão de 20 de outubro de 2022, Digi, C 77/21, EU:C:2022:805, nº 49 e jurisprudência referida). O responsável pelo tratamento deve poder demonstrar o respeito por esses princípios, em conformidade com o princípio da responsabilidade enunciado no artigo 5.º, n.º 2, do referido regulamento (v., neste sentido, Acórdão de 20 de outubro de 2022, Digi, C 77/21, EU:C:2022:805, nº 24).

Pelos fundamentos expostos, a Primeira Secção TJUE, declarou na decisão de 07/12/2023:

> O artigo 22, nº 1, do [...] [RGPD], relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados [...],
>
> deve ser interpretado no sentido de que:
>
> a determinação automatizada, por uma sociedade que fornece informações comerciais, de um valor de probabilidade baseado em dados pessoais relativos a uma pessoa sobre a capacidade desta para cumprir as suas obrigações de pagamento no futuro constitui

> uma «decisão individual automatizada», na acepção desta disposição, quando o facto de um terceiro, ao qual o referido valor de probabilidade é comunicado, estabelecer, executar ou cessar uma relação contratual com essa pessoa depende de forma determinante desse valor de probabilidade.

A interpretação do artigo 22, nº 1, do RGPD, como se vê da decisão, faculta ao titular dos dados o direito de não aceitar a uma decisão baseada exclusivamente no tratamento automatizado, incluindo a definição de perfis. O uso de um escore de crédito de IA para aprovação de crédito a ser dado por terceiro poderá ser considerada uma decisão se desempenhar um papel decisivo na tomada da decisão. O cálculo de solvência fornecidos por empresas de pontuação de crédito não constitui, em princípio, uma decisão individual automatizada na acepção do RGPD, mas sim um auxílio à tomada de decisão, uma vez que a decisão em si, como por exemplo recusar uma compra a prazo, se for tomada apenas pelos clientes que usam o relatório para dar ou não um crédito ao titular dos dados.

Caso Avanza Bank AB: dados pessoais transferidos para o Facebook (Decisão DI-2021-5544, IMY 2024, Suécia)

A Autoridade Sueca de Proteção à Privacidade (IMY) é a agência governamental da Suécia responsável por supervisionar a aplicação do RGPD, velando para que as pessoas estejam protegidas contra a violação da sua privacidade pessoal pelo processamento dos seus dados, monitorando para que eles sejam tratados corretamente e não caiam em mãos não autorizadas. Sua missão é:

> Trabalhar para garantir que os direitos e liberdades

> fundamentais das pessoas sejam protegidos no processamento de dados pessoais, para facilitar a livre circulação de tais dados dentro da União Europeia e trabalhar para garantir que boas práticas sejam observadas nas atividades de classificação de crédito (IMY, 2025).

Segundo relatado na decisão DI-2021-5544, de 2024, no dia 08/06/2021, o IMY recebeu uma notificação de violação de dados pessoais contra o *Avanza Bank AB*, um banco *online* sueco com sede em Estocolmo, especializado em poupança, investimentos e pensões, revelando que dados pessoais de meio a um milhão de clientes haviam sido transferidos indevidamente para o Facebook, agora Meta, no período de 15/11/ 2019 a 02/06/2021. Entre as informações pessoais transferidas estavam o número de identificação de beneficiário da previdência social, valor de empréstimo e número de conta bancária (IMY,2024).

O incidente do caso ocorreu quando o banco começou a usar o serviço "Pixel do Facebook", agora Pixel Meta, para otimizar o marketing do banco. O Facebook desenvolveu em 2019 o recurso denominado *Automatic Advanced Matching* (AAM) (IMY, 2024).

O Pixel da Meta, como se vê no site (META, 2025) é um trecho de código instalado no site do interessado que pode ajudar a verificar a eficácia da publicidade e as ações que as pessoas realizam no site, como visitar uma página ou adicionar um item ao carrinho, também ver quando os clientes realizarem uma ação após ver um anúncio no Facebook e no Instagram (IMY, 2024).

No relatório da decisão (DI-2021-5544, 2024), a transferência incorreta de dados pessoais dos clientes do banco foi causada pelo recurso AAM, que fora ativado por engano por pessoa do banco. Ao tomar conhecimento do incidente da transferência de dados, por meio de informações externas, o banco desativou o Pixel

da Meta em sua totalidade (IMY, 2024).

À luz das informações contidas na notificação da violação de dados pessoais, o IMY iniciou a investigação do caso para verificar se o banco havia tomado as medidas técnicas e organizativas adequadas para proteger os dados pessoais, em conformidade com o artigo 5.º sobre os princípios relativos ao processamento de dados pessoais, n.º 1, alínea f), e o artigo 32, sobre a segurança do processamento, n.º 1, do RGPD, no período do incidente 15/11/2019 à 02/06/2021 (IMY, 2024).

Depois de ter ciência da transferência indevida de dados para a Meta, o banco revisou seus procedimentos internos para garantir o processamento correto e seguro de dados pessoais dos clientes (IMY, 2024).

A decisão do IMY (2024), imputou ao banco a responsabilidade pela violação do RGPD, por não ter tomado as medidas técnicas e organizacionais apropriadas para garantir um nível adequado de segurança para os dados pessoais dos clientes, e aplicou uma multa administrativa de aproximadamente um milhão e trezentos mil euros, com fundamento nos dispositivos citados acima e no artigo 83.º do RGPD, que dispõe sobre as condições gerais para a imposição de multas administrativas.

Caso CK vs. Magistrat Der Stadt Wien, interveniente Dun & Bradstreet Austria GMBH: "scoring" para tratamento de dados pessoais, Áustria (TJUE C-203/22, 2025)

Segundo o relatório do juiz Thomas von Danwitz do TJUE, a *Dun & Bradstreet Austria GmbH* (D&B), empresa especializada na realização de avaliações de crédito austríaca, prestou informações para uma operadora de telecomunicações móveis, que resultaram na

recusou a CK para celebração ou a prorrogação de um contrato de telecomunicações móveis que implicava o pagamento mensal do montante de 10 euros, com o fundamento de que, segundo a avaliação automatizada de crédito, aquele não dispunha de solvência financeira suficiente (UNIÃO EUROPEIA, 2025).

CK recorreu à autoridade austríaca para a proteção de dados, que ordenou à D&B que prestasse a ele informações úteis relativas à lógica subjacente à decisão automatizada com base nos seus dados pessoais. A decisão foi favorável e determinou que a D&B prestasse a CK informações úteis relativas à lógica subjacente a definição do seu perfil com base nos seus dados pessoais (UNIÃO EUROPEIA, 2025).

A D&B interpôs recurso da decisão dessa autoridade para o Tribunal Administrativo Federal da Áustria, alegando, em substância, que, por razões de segredo comercial protegido, não tinha de prestar a CK informações adicionais às que já lhe tinham sido prestadas (UNIÃO EUROPEIA, 2025).

Por Decisão de 23/10/2019 o Tribunal Administrativo Federal da Áustria declarou que a D&B tinha violado o artigo 15, nº 1, alínea h), do RGPD ao não prestar a CK informações úteis relativas à lógica subjacente à decisão automatizada sobre os dados pessoais de CK ou, pelo menos, ao não fundamentar suficientemente a alegada impossibilidade em que se encontrava de prestar essas informações (UNIÃO EUROPEIA, 2025).

O artigo 15 do RGPD, sob a epígrafe “Direito de acesso do titular dos dados”, tem a seguinte redação:

> 1. O titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de

> aceder aos seus dados pessoais e às seguintes informações:
>
> […];
>
> h) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22, nº 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.

Em especial, segundo o relatório da decisão, o Tribunal Administrativo Federal da Áustria salientou que a D&B não tinha dado explicações suficientes a CK que lhe permitissem compreender de que modo tinha sido feito, a seu respeito, o prognóstico sobre a probabilidade do seu comportamento futuro com relação ao não pagamento da conta de telefonia, o que esta empresa lhe comunicou com o pormenor de que, para obter esse escore, tinham sido "agregados de forma equivalente" certos dados sociodemográficos de CK (UNIÃO EUROPEIA, 2025).

A decisão de 2019 do Tribunal Administrativo Federal da Áustria transitou em julgado. No entanto, o pedido de execução coerciva desta decisão, apresentado por CK à Administração Municipal de Viena, autoridade de execução, foi indeferido com o fundamento de que a D&B já tinha cumprido suficientemente o seu dever de informação, apesar de esta empresa não ter fornecido nenhuma informação adicional após a decisão do Tribunal Administrativo Federal da Áustria (UNIÃO EUROPEIA, 2025).

Então, CK interpôs recurso da decisão da Administração Municipal de Viena, primeira instância, para o Tribunal Administrativo de Viena, segunda instância, com vista à execução coerciva da decisão de 2019 do Tribunal Administrativo Federal da Áustria, que considerou, por força do direito austríaco, a obrigação

da execução da última decisão, o que implicava determinar os atos concretos que a D&B era obrigada a praticar por força dessa decisão da alta corte (UNIÃO EUROPEIA, 2025).

Por considerar que a determinação só poderia ser efetuada por um perito com as competências necessárias, o Tribunal Administrativo de Viena nomeou um perito, o qual considerou que a D&B, para cumprir o seu dever para com CK, teria de prestar as seguintes informações mínimas:

- os dados pessoais de CK que foram tratados no âmbito da constituição de um «fator» (data de nascimento, endereço, sexo etc.);
- a fórmula matemática que está na base do cálculo que conduziu ao «score» em causa no processo principal;
- o valor concreto atribuído a CK por cada um dos fatores em causa, e
- a indicação específica dos intervalos dentro dos quais o mesmo valor é atribuído a diferentes dados para o mesmo fator (avaliação por intervalos ou avaliação discreta ou indiciária/cadastral) (UNIÃO EUROPEIA, 2025).

Para garantir que, após a sua comunicação, a exatidão dessas informações mínimas pudesse ser verificada por CK, a D&B deveria igualmente fornecer uma lista indicativa dos escores de pessoas para o período que abrangesse os seis meses anteriores e os seis meses subsequentes à definição do escore de CK e que foram obtidos com base na mesma regra de cálculo aplicado a CK (UNIÃO EUROPEIA, 2025).

Segundo o Tribunal Administrativo de Viena, só a comunicação das informações mínimas identificadas pelo referido

perito permitiria verificar a coerência e a exatidão das informações prestadas pelo responsável que fez o tratamento nos termos do artigo 15, nº 1, alínea h), do RGPD (UNIÃO EUROPEIA, 2025).

No caso, vários indícios mostravam claramente que as informações prestadas pela D&B eram contrárias aos fatos. Com efeito, embora as informações comunicadas a CK, entre as quais, nomeadamente, o escore obtido, comprovassem uma elevada solvência por parte dele, a definição de perfil real levou a considerar que ela não era solvente para o pagamento de dez euros por mês no âmbito de um contrato de telecomunicações móveis (UNIÃO EUROPEIA, 2025).

O Tribunal Administrativo de Viena considerou que se apresentava a questão de saber se o artigo 15, nº 1, alínea h), do RGPD garantiria ao titular dos dados a possibilidade de verificar a exatidão das informações comunicadas pelo responsável que fez o tratamento dos dados, a D&B no caso. Colocou-se igualmente a questão de saber se e em que medida a exceção relativa à existência de um segredo comercial é suscetível de restringir esse direito de acesso garantido pelas disposições conjugadas do artigo 15, nº 1, alínea h), e do artigo 22 do RGPD. Nestas circunstâncias, o Tribunal Administrativo de Viena decidiu suspender a instância e submeter ao TJUE questões prejudiciais quanto a interpretação do RGPD (UNIÃO EUROPEIA, 2025).

Cabe informar que uma questão prejudicial ao TJUE é um procedimento que permite aos tribunais nacionais dos Estados-Membros da UE solicitar uma decisão sobre a interpretação ou validade do direito da UE, quando esta questão é fundamental para a resolução de um caso pendente perante eles; é um incidente de instância num processo judicial nacional onde a resolução de um litígio depende do esclarecimento sobre uma norma de Direito da UE.

No TJUE foram invocados os seguintes princípios para a solução do caso:

> Os considerandos 4, 11, 58, 63 e 71 do RGPD enunciam:
>
> (4) O tratamento dos dados pessoais deverá ser concebido para servir as pessoas. O direito à proteção de dados pessoais não é absoluto; deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade. O presente regulamento respeita todos os direitos fundamentais e observa as liberdade e os princípios reconhecidos na [Carta dos Direitos Fundamentais da União Europeia (a seguir "Carta")], consagrados nos Tratados, nomeadamente o respeito pela vida privada e familiar, pelo domicílio e pelas comunicações, a proteção dos dados pessoais, a liberdade de pensamento, de consciência e de religião, a liberdade de expressão e de informação, a liberdade de empresa, o direito à ação e a um tribunal imparcial, e a diversidade cultural, religiosa e linguística;
>
> […];
>
> (11) A proteção eficaz dos dados pessoais na União Europeia exige o reforço e a especificação dos direitos dos titulares dos dados e as obrigações dos responsáveis pelo tratamento e pela definição do tratamento dos dados pessoais, bem como poderes equivalentes para controlar e assegurar a conformidade das regras de proteção dos dados pessoais e sanções equivalentes para as infrações nos Estados-Membros;
>
> […];
>
> (58) O princípio da transparência exige que qualquer informação destinada ao público ou ao titular dos dados seja 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;

[…];

(63) Os titulares de dados deverão ter o direito de aceder aos dados pessoais recolhidos que lhes digam respeito e de exercer esse direito com facilidade e a intervalos razoáveis, a fim de conhecer e verificar a tomar conhecimento do tratamento e verificar a sua licitude. […] Esse direito não deverá prejudicar os direitos ou as liberdades de terceiros, incluindo o segredo comercial ou a propriedade intelectual e, particularmente, o direito de autor que protege o software. Todavia, essas considerações não deverão resultar na recusa de prestação de todas as informações ao titular dos dados;

[…];

(71) O titular dos dados deverá ter o direito de não ficar sujeito a uma decisão, que poderá incluir uma medida, que avalie aspetos pessoais que lhe digam respeito, que se baseie exclusivamente no tratamento automatizado e que produza efeitos jurídicos que lhe digam respeito ou o afetem significativamente de modo similar, como a recusa automática de um pedido de crédito por via eletrônica ou práticas de recrutamento eletrônico sem qualquer intervenção humana. Esse tratamento inclui a definição de perfis mediante qualquer forma de tratamento automatizado de dados pessoais para avaliar aspetos pessoais relativos a uma pessoa singular, em especial a análise e previsão de aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados, quando produza efeitos jurídicos que lhe digam respeito ou a afetem significativamente de forma similar […]. Em qualquer dos casos, tal tratamento deverá ser acompanhado das garantias

> adequadas, que deverão incluir a informação específica ao titular dos dados e o direito de obter a intervenção humana, de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação e de contestar a decisão. […].

Sabemos que os considerandos não têm força vinculante na aplicação da norma da UE, mas constituem um elemento interpretativo. Como se vê do guia para a redação de textos legislativos da EU, os considerandos fundamentam os regulamentos, diretivas e decisões. Tem por finalidade dar a conhecer as circunstâncias em que o RGPD, no caso, foi promulgado e dar a possibilidade às partes em litígio de defender os seus direitos, bem como ao TJUE de exercer a sua fiscalização jurisdicional (UNIÃO EUROPEIA, 2016).

Pelos fundamentos expostos no julgamento, ao final, a Primeira Secção TJUE declarou, em 27/02/2025, que:

> 1) O artigo 15, nº 1, alínea h), do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), deve ser interpretado no sentido de que:
>
> no caso de decisões automatizadas, incluindo a definição de perfis, na acepção do artigo 22, nº 1, deste regulamento, o titular dos dados pode exigir do responsável pelo tratamento, a título de «informações úteis relativas à lógica subjacente», que este lhe explique, através de informações pertinentes e de forma concisa, transparente, inteligível e de fácil

> acesso, o procedimento e os princípios concretamente aplicados para explorar, por via automatizada, os dados pessoais relativos a essa pessoa com vista a obter um determinado resultado, como um perfil de solvência.
>
> 2) O artigo 15, nº 1, alínea h), do Regulamento 2016/679 deve ser interpretado no sentido de que:
>
> na hipótese de o responsável pelo tratamento considerar que as informações a prestar ao titular dos dados em conformidade com esta disposição contêm dados de terceiros protegidos por este regulamento ou relativos a segredo comercial, na acepção do artigo 2, ponto 1, da Diretiva (UE) 2016/943 do Parlamento Europeu e do Conselho, de 8 de junho de 2016, relativa à proteção de *know-how* e de informações comerciais confidenciais (segredos comerciais) contra a sua aquisição, utilização e divulgação ilegais, esse responsável é obrigado a comunicar as informações alegadamente protegidas à autoridade de controlo ou ao órgão jurisdicional competentes, aos quais incumbe ponderar os direitos e os interesses em causa para determinar o alcance do direito de acesso do titular dos dados previsto no artigo 15 deste regulamento (UNIÃO EUROPEIA, 2025).

Segundo Diana Camões cabe a reflexão sobre o alcance do "direito à explicação". Porque os sistemas de IA são caracterizados pela falta de transparência, o que dificulta em muitos casos a plena compreensão das decisões adotadas pela classificação de crédito. Conforme a decisão acima, para os efeitos do RGPD, na adoção de uma decisão individual automatizada, o titular dos dados pode exercer os direitos previstos no artigo 22.º, de obter a intervenção humana na avaliação, manifestar o seu ponto de vista e contestar a decisão da negativa de concessão do crédito. Pois este artigo 22.º não prevê, expressamente, o direito à explicação da decisão. A única

menção é feita, como se vê acima, no considerando (71) do RGPD, de acordo com o qual o titular dos dados pode obter uma explicação. Este foi o principal argumento invocado na doutrina por autores como Bryce Goodman (Goodman: *Discrimination, data sanitisation and auditing in the european union's general data protection regulation, 2016*) e Seth Flaxman (Goodman and Flaxman, Oxford: *European Union regulations on algorithmic decision-making and a "right to explanation"*). Assim, a consagração do direito à explicação está inserida no âmbito das garantias adequadas de proteção para o titular dos dados (CAMÕES, 2025).

O dever em relação ao qual a D&B, responsável pelo tratamento, se encontra obrigada não estará cumprido pela mera comunicação de uma fórmula matemática complexa, um algoritmo, nem com a descrição detalhada de todas as etapas da decisão automatizada. Evidentemente o conhecimento geral dos titulares de dados não são especializados em IA ou em Matemática Algorítmica, razão pela qual a explicação fornecida no início do caso não foi inteligível (CAMÕES, 2025).

Na análise do caso, este é o ponto mais importante da decisão do TJUE, em tela. Segundo Diana Camões "pela primeira vez, o TJ deixa claro que o direito à explicação não é uma mera formalidade, devendo ser acompanhado de uma explicação lógica, efetiva e transparente sobre os critérios aplicados durante o processo da tomada de decisão, de forma a garantir que o titular dos dados consiga, efetivamente, compreender o seu conteúdo" (CAMÕES, 2025).

O TJUE expressa, na argumentação do juiz Thomas von Danwitz, relator do julgado, que a explicação deverá ser acompanhada de uma descrição do procedimento e dos princípios concretamente aplicados, para que o titular dos dados possa entender quais os seus dados pessoais que foram utilizados no momento da decisão automatizada em causa, bem como os meios que foram

adotados. Durante vários anos, a doutrina que defendia a existência do direito à explicação baseava a sua posição no considerando (71) do RGPD, algo que merecia críticas de vários autores pela sua ausência de caráter vinculativo do texto (CAMÕES, 2025), especialmente Goodman e Flaxman, de Oxford – *European Union regulations on algorithmic decision-making and a "right to explanation"*.

O TJUE reconheceu que a explicação fornecida ao titular dos dados terá de ser efetiva, não bastando aos responsáveis pelo tratamento o fornecimento de uma informação abstrata e de uma mera fórmula matemática, pois a IA tem entre as características ser como uma caixa preta, especialmente na *deep learning*, sem possibilidade de que se tenha o devido conhecimento do funcionamento dos sistemas algorítmicos. Com a decisão do caso C-203/22, em 2025, os responsáveis pelo tratamento de dados deverão repensar as suas políticas de pontuação de crédito (CAMÕES, 2025).

CONCLUSÃO

A jornada crítica traçada neste artigo culmina numa constatação fundamental: a pontuação de crédito, em sua versão atual e automatizada, já não é apenas uma ferramenta exclusivamente financeira, mas sim uma prática social com implicações profundas sobre inclusão, cidadania digital e governança de dados. Em um mundo cada vez mais mediado por tecnologias inteligentes, o acesso ao crédito tornou-se uma espécie de barreira invisível que separa oportunidades e determina destinos – muitas vezes sem que os indivíduos compreendam ou sequer saibam que critérios estão sendo avaliados.

É nesse contexto que se impõe a necessidade de repensar os

sistemas de escore de crédito à luz dos princípios éticos e jurídicos que regem as sociedades democráticas. A evolução da inteligência artificial, com suas promessas de eficiência e personalização, não pode eclipsar os valores de transparência, equidade e respeito aos direitos fundamentais. Modelos preditivos sofisticados – como redes neurais profundas e algoritmos de conjunto – devem ser acompanhados por mecanismos de explicabilidade e supervisão humana. A tendência de opacidade dos sistemas de inteligência artificial, conhecida como "caixa preta algorítmica", precisa ser enfrentada com coragem regulatória e compromisso ético.

Os estudos de caso analisados reforçam essa necessidade. Na Alemanha, o caso Schufa evidenciou que o escore de crédito pode ter impacto decisivo nas relações contratuais, exigindo, por consequência, o cumprimento dos requisitos previstos pelo RGPD. Na Áustria, o TJUE consolidou o entendimento de que o direito à explicação deve ser concreto e inteligível, não sendo suficiente a apresentação de fórmulas matemáticas abstratas. Já na Suécia, a penalização do Avanza Bank pelo vazamento de dados demonstra como a governança de dados e a escolha de parceiros tecnológicos são essenciais na conformidade com a proteção da privacidade.

No Brasil, embora o escore de crédito seja considerado lícito, a ausência de um marco regulatório específico, somado à ampla margem de interpretação da LGPD, cria zonas de insegurança jurídica que fragilizam o consumidor. A jurisprudência do STJ, ao pacificar temas como o direito à informação e os limites do segredo comercial, avança na consolidação de direitos, mas ainda não resolve a questão da transparência algorítmica e da legitimidade dos cálculos realizados. O caso XP reforça a responsabilidade objetiva das instituições na proteção dos dados, especialmente quando há terceirização dos serviços de armazenamento.

Do ponto de vista ético, a pontuação de crédito por IA exige uma abordagem centrada no ser humano. Os riscos de discriminação

por raça, gênero, condição econômica ou histórico pessoal são reais e precisam ser mitigados com medidas proativas, como auditoria dos modelos, uso de conjuntos de dados representativos e implementação de sistemas de supervisão. O respeito à autodeterminação informacional – isto é, o direito do indivíduo de controlar como seus dados são usados – deve ser o norte de qualquer prática creditícia automatizada. E, nesse sentido, a criação de comitês de ética, canais de reclamação e mecanismos de revisão humana são elementos que fortalecem a confiança entre consumidores e instituições.

O artigo também destaca que a pontuação de crédito por IA pode ser uma aliada da inclusão financeira, especialmente ao considerar dados alternativos de populações historicamente excluídas do sistema de crédito tradicional. Diaristas, trabalhadores informais, empreendedores autônomos – todos esses grupos podem ser contemplados por modelos mais flexíveis e responsivos. No entanto, essa inclusão só se concretiza se os sistemas forem acompanhados por normas de transparência, segurança e proporcionalidade. Sem isso, a IA corre o risco de perpetuar ou aprofundar desigualdades, ao invés de reduzi-las.

Por fim, o futuro do escore de crédito está intimamente ligado à capacidade das sociedades de harmonizarem a inovação tecnológica com responsabilidade social. A convergência entre IA, *blockchain*, PLN e outras tecnologias emergentes precisa ser acompanhada por estruturas regulatórias dinâmicas, capazes de acompanhar os avanços e corrigir as distorções. O papel dos órgãos reguladores, da sociedade civil e dos próprios consumidores é fundamental nessa construção. É preciso incentivar a alfabetização digital, promover o debate público sobre algoritmos e garantir que cada indivíduo possa compreender e contestar a forma como é avaliado.

REFERÊNCIAS

ADDY, W. A. *et al*. "AI in credit scoring: A comprehensive review of models and predictive analytics". **Global Journal of Engineering and Technology Advances**, vol. 18, 2024.

ALIREZAIE, M. *et al*. "Decentralized data and artificial intelligence orchestration for transparent and efficient small and medium-sized enterprises trade financing". **Journal of Risk and Financial Management**, vol. 17, 2024.

BABAWURUN, T. *et al*. "A comprehensive review of wind turbine modeling for addressing energy challenges in Nigeria and South Africa in the 4IR context". **The Journal of Engineering and Exact Sciences**, vol. 9, n. 2, 2023.

BRASIL. "Encontre uma instituição regulada/supervisionada pelo BCB". **BCB** [2025]. Disponível em: <www.bcb.gov.br>. Acesso em: 15/09/2026.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília: Planalto, 1988. Disponível em: <www.planalto.gov.br>. Acesso em: 15/09/2026.

BRASIL. **Decreto-Lei n. 73, de 21 de novembro 1966**. Brasília: Conselho Monetário Nacional, 1966. Disponível em: <www.cmn.gov.br>. Acesso em: 15/09/2026.

BRASIL. **Lei Complementar n. 105, de 10 de janeiro de 2001**. Brasília: Conselho Monetário Nacional, 2001. Disponível em: <www.cmn.gov.br>. Acesso em: 15/09/2026.

BRASIL. **Lei n. 4.595, de 31 de dezembro de 1964**. Brasília: Planalto, 1964. Disponível em: <www.planalto.gov.br>. Acesso em: 15/09/2026.

BRASIL. **Lei n. 5.869, de 11 de janeiro de 1973**. Brasília: Planalto, 1973. Disponível em: <www.planalto.gov.br>. Acesso em: 15/09/2026.

BRASIL. **Lei n. 8.078, de 11 de setembro de 1990**. Brasília: Planalto, 1990. Disponível em: <www.planalto.gov.br>. Acesso em: 15/09/2026.

BRASIL. **Lei n. 12.414, de 9 de junho de 2011**. Brasília: Planalto, 2011. Disponível em: <www.cmn.gov.br>. Acesso em: 15/09/2026.

BRASIL. **Lei n. 12.965, de 23 de abril de 2014**. Brasília: Planalto, 2014. Disponível em: <www.planalto.gov.br>. Acesso em: 15/09/2026.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Brasília: Planalto, 2018. Disponível em: <www.planalto.gov.br>. Acesso em: 15/09/2026.

BRASIL. **Lei n. 13.853, de 8 de julho de 2019**. Brasília: Planalto, 2019. Disponível em: <www.planalto.gov.br>. Acesso em: 15/09/2026.

BRASIL. **Resolução n. 342, de 26 de setembro 2023**. Brasília: Conselho Monetário Nacional, 2024. Disponível em: <www.cmn.gov.br>. Acesso em: 15/09/2026.

BRASIL. **Resolução n. 4.571, de 26 maio 2017**. Brasília: Conselho Monetário Nacional, 2017. Disponível em: <www.cmn.gov.br>. Acesso em: 15/09/2026.

BRASIL. **Resolução n. 4.658, de 26 de abril de 2018**. Brasília: Conselho Monetário Nacional, 2018. Disponível em: <www.cmn.gov.br>. Acesso em: 15/09/2026.

BRASIL. **Resolução n. 4.893, de 26 de fevereiro 2021**. Brasília: Conselho Monetário Nacional, 2021. Disponível em: <www.cmn.gov.br>. Acesso em: 15/09/2026.

BRASIL. **REsp 1.197.929-PR**. Relator: Ministro Luis Felipe Salomão. Data: 12/09/2011. Brasília: Superior Tribunal de Justiça, 2011. Disponível em: <www.stj.jus.br>. Acesso em: 15/09/2026.

BRASIL. **REsp 2.015.732-SP**. Relatora: Nancy Andrighi. Data: 20/06/2023. Brasília: Superior Tribunal de Justiça, 2023. Disponível em: <www.stj.jus.br>. Acesso em: 15/09/2026.

BRASIL. **REsp. 1.149.998-RS**. Relatora: Nancy Andrighi. Data: 07/08/2012. Brasília: Superior Tribunal de Justiça, 2012. Disponível em: <www.stj.jus.br>. Acesso em: 15/09/2026.

BRASIL. **REsp. 1.995.458-SP**. Relatora: Nancy Andrighi. Data: 09/08/2022. Brasília: Superior Tribunal de Justiça, 2022. Disponível em: <www.stj.jus.br>. Acesso em: 15/09/2026.

BRASIL. **REsp. 2.077.278-SP**. Relatora: Nancy Andrighi. Data: 09/10/2023. Brasília: Superior Tribunal de Justiça, 2023. Disponível em: <www.stj.jus.br>. Acesso em: 15/09/2026.

BRASIL. **REsp. n. 1.419.697-RS**. Relator: Paulo de Tarso Sanseverino. Data: 12/11/2014. Brasília: Superior Tribunal de Justiça, 2014. Disponível em: <www.stj.jus.br>. Acesso em: 15/09/2026.

BRASIL. **Sistema de Informações de Créditos**. Brasília: Banco Central, 2024. Disponível em: <www.bcb.gov.br>. Acesso em: 15/09/2026.

BRASIL. **Súmula 479**. Brasília: Superior Tribunal de Justiça, 2012. Disponível em: <www.stj.jus.br>. Acesso em: 15/09/2026.

BRASIL. **Tema Repetitivo 466**. **Origem**: REsp 1.197.929-PR. Relator: Ministro Luis Felipe Salomão. Data: 12/09/2011. Brasília: Superior Tribunal de Justiça, 2011. Disponível em: <www.stj.jus.br>. Acesso em: 15/09/2026.

ÇALLI, B. A.; COŞKUN, E. "A longitudinal systematic review of credit risk assessment and credit default predictors". **Sage Journals**, vol. 11, 2021.

CAMÕES, D. **O direito à explicação no RGPD**: o fim da querela doutrinal? Lisboa: Universidade de Lisboa, 2025.

CHATTERJEE, S. *et al*. "A quantitative theory of the credit score". **Econometrica Journal of the Econometrics Society**, vol. 91. n. 5. 2023.

CHIU, I. H. Y.; LIM, E. "Technology vs ideology: how far will artificial intelligence and distributed ledger technology transform corporate governance and business?" **Berkeley Business Law Journal**, vol. 18, n. 1, 2020.

CONSELHO DA EUROPA. **Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais**. Roma: Conselho Europeu, 1950.

DASHOTTAR, S.; SRIVASTAVA, V. "Corporate banking-risk management, regulatory and reporting framework in India: a

blockchain application-based approach". **Journal of Banking Regulation**, vol. 22, 2021.

DUMITRESCU, E. I. *et al*. "Machine learning for credit scoring: improving logistic regression with non-linear decision-tree effects". **European Journal of Operational Research**, vol. 297, 2022.

DWIVEDI, R. *et al*. "Explainable AI (XAI): Core Ideas, Techniques and Solutions". **ACM Computing Surveys**, vol. 55, 2023.

FRITZ-MORGENTHAL, S.; HEIN, B.; PAPENBROCK, J. "Financial Risk Management and Explainable, Trustworthy, Responsible AI". **Frontiers in Artificial Intelligence**, vol. 5, 2022.

GICIĆ, A.; ĐONKO, D.; SUBASI, A. "Intelligent credit scoring using deep learning methods". **Concurrency and Computation: Practice and Experience**, vol. 35, 2023.

GOLBAYANI, P.; FLORESCU, I.; CHATTERJEE, R. "A comparative study of forecasting corporate credit ratings using neural networks, support vector machines, and decision trees". **The North American Journal of Economics and Finance**, vol. 54, 2020.

GONÇALVES, C. G. B. **Direito fundamental à proteção de dados pessoais a responsabilidade civil por desvio de finalidade da proteção ao crédito no uso do score para fins discriminatórios ao consumidor** (Dissertação de Mestrado em Direito Constitucional). Brasília: UnB, 2022.

IMY. "About us". **IMY** [2025]. Disponível em: <www.imy.se>. Acesso em: 15/09/2026.

IMY. “Beslut efter tillsyn enligt dataskyddsförordningen mot Avanza Bank AB”. **IMY** [2024]. Disponível em: <www.imy.se>. Acesso em: 15/09/2026.

INVESTOPEDIA. “About Us”. **Investopedia** [2025]. Disponível em: <www.investopedia.com>. Acesso em: 07/09/2026.

JONES, L. A.; HILLER, J. S. “Who's Keeping score: oversight of changing consumer credit infrastructure”. **American Business Law Journal**, vol. 59, n. 1, 2022.

KAPLAN, B.; BENLI, V. F.; ALP, E. A. “Blockchain based decentralized lending protocols: a return analysis between S&P 500 and DeFi assets”. **Journal of Emerging Economies And Policy**, vol. 8, 2023.

LAINEZ, N.; GARDNER, J. “Algorithmic credit scoring in vietnam: a legal proposal for maximizing benefits and minimizing risks”. **Asian Journal of Law and Society**, vol. 10, 2023.

LESCRAUWAET, L. *et al*. Adaptive legal frameworks and economic dynamics in emerging technologies: navigating the intersection for responsible innovation”. **Law and Economics**, **Institute for Law and Economics Studies**, vol. 16, 2022.

MAGNUSON, W. J. “Artificial financial intelligence”. **Harvard Business Law Review**, vol. 10, n. 2, 2020.

META. “Pixel da Meta: adicione um trecho de código ao seu site com o qual você pode mensurar, otimizar e criar públicos para suas campanhas de anúncios”. **Facebook** [2025]. Disponível em: <www.facebook.com>. Acesso em: 16/09/2026.

MIGALHAS. “Juiz de SC extingue cerca de 55 mil processos sobre credit scoring por meio de portaria”. **Migalhas** [2025]. Disponível em: <www.migalhas.com.br>. Acesso em: 16/09/2026.

MUBARAK, H. *et al*. “Improved active and reactive energy forecasting using a stacking ensemble approach: steel industry case study”. **Energies**, vol. 16, 2023.

OLIVEIRA, C. A. A. **Comentários ao Código de Processo Civil**: arts. 796 a 889. Rio de Janeiro: Editora Forense, 2002.

PETERS, D. *et al*. “Responsible AI-Two frameworks for ethical design practice”. **IEEE Transactions on Technology and Society**, vol. 1, n. 1, 2020.

PIMENTEL, L. O.; RASZL PIMENTEL, H. **Sistema financeiro**: escore de crédito, tratamento e proteção de dados pessoais na União Europeia. Braga: Conpedi, 2025.

RATZAN, J.; RAHMAN, N. “Measuring responsible artificial intelligence (RAI) in banking: a valid and reliable instrument”. **AI and Ethics**, vol. 4, 2024.

SANDRONI, P. (org.) **Novíssimo dicionário de economia**. São Paulo: Editora Best Seller, 1999.

SCHUFA. “Über uns”. **Schufa** [2025]. Disponível em: <www.schufa.de>. Acesso em: 14/09/2026.

SERASA EXPERIAN. “A Serasa Experian”. **Serasa Experian** [2025]. Disponível em: <www.serasaexperian.com.br>. Acesso em: 14/09/2026.

SETH, A. “Ethical issues in artificial intelligence: towards fairness, bias and accountability in AI system”. **International Journal of Advancements in Computational Technology**, vol. 2, n. 2, 2024.

SILVA, P. **Vocabulário jurídico**. Rio de Janeiro: Editora Forense, 2014.

TALAAT, F. M. *et al*. “Toward interpretable credit scoring: integrating explainable artificial intelligence with deep learning for credit card default prediction”. **Neural Computing and Applications**, vol. 36, 2023.

TANNA, M.; DUNNING, W. “Bias and discrimination in the use of AI in the financial sector”. *In*: REMOLINA, N.; GURREA-MARTINEZ, A. (eds.). **Artificial intelligence in finance**: challenges, opportunities and regulatory developments. Cheltenham: Edward Elgar Publishing, 2023.

ȚÎRCOVNICU, G. I.; HAȚEGAN, C. D. “The Audit Risk Assessment of European Small- and Mid-Size Enterprises”. **Journal of Risk and Financial Management**, vol. 16, 2023.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais**. Paris: União Europeia, 2000. Disponível em: <www.european-union.europa.eu>. Acesso em: 15/09/2026.

UNIÃO EUROPEIA. **Guia prático comum do Parlamento Europeu, do Conselho e da Comissão para as pessoas que contribuem para a redação de textos legislativos da União Europeia**. Bruxelas: União Europeia, 2016. Disponível em: <www.european-union.europa.eu>. Acesso em: 15/09/2026.

UNIÃO EUROPEIA. **Processo C-203/22**. Relator: Thomas von Danwitz. Data: 27/02/2025. Bruxelas: Tribunal de Justiça União

Europeia, 2025. Disponível em: <www.european-union.europa.eu>. Acesso em: 15/09/2026.

UNIÃO EUROPEIA. **Processo C-634/21**. Relator: Andreas Kumin. Data: 07/12/2023. Bruxelas: Tribunal de Justiça União Europeia, 2025. Disponível em: <www.european-union.europa.eu>. Acesso em: 15/09/2026.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679, de 27 abril de 2016**. Bruxelas: União Europeia, 2016. Disponível em: <www.european-union.europa.eu>. Acesso em: 15/09/2026.

UZOUGBO, N. S.; IKEGWU, C. G.; ADEWUSI, A. O. "Legal accountability and ethical considerations of AI in financial services". **GSC Advanced Research and Reviews**, vol. 19, 2024.

WISE. "TransferWise Brasil Corretora de Câmbio". **WISE** [2025]. Disponível em: <www.wise.com>. Acesso em: 08/09/2026.

WULF, A. J.; SEIZOV, O. "Please understand we cannot provide further information: evaluating content and transparency of RGPD-mandated AI disclosures". **AI & Society: Knowledge, Culture and Communication**, vol. 39, 2024.

ZAKI, A. M. *et al*. "Predictive analytics and machine learning in direct marketing for anticipating bank term deposit subscriptions". **American Journal of Business and Operations Research**, vol. 11, 2024.