Capítulo 19

O Uso de Biometria na Formalização de Contratos Eletrônicos à Luz da Lei Geral de Proteção de Dados Pessoais

The Use of Biometry in the Formalization of Electronic Contracts in Light of the General Law on the Protection of Personal Data

Cezar Augusto de Sousa Santos

Pós-graduado Lato Sensu em Direito Contratual pela Pontifícia Universidade Católica de São Paulo – PUC/SP (2024). Graduado em Direito pelo Centro Universitário das Faculdades Metropolitanas Unidas – FMU (2019).

Ronny Max Machado

Mestre em Direito da Sociedade da Informação pelo Centro Universitário das Faculdades Metropolitanas Unidas. São Paulo. Estado de São Paulo. Brasil. Coordenou o Grupo de Pesquisa em Privacidade de Dados junto ao Programa Empreendireito da Faculdade de Direito da Universidade Presbiteriana Mackenzie. Estado de São Paulo. Brasil.2018-2019. Pesquisador junto ao Programa de Mestrado em Direito da Sociedade da Informação pelo Centro Universitário das Faculdades Metropolitanas Unidas, São Paulo. Estado de São Paulo. Brasil. Diretor de Pesquisa e pesquisador junto à Liga Acadêmica Brasileira de Antropologia e Direito Indígena - LABADI (2022-2023). Professor universitário dos cursos de pós-graduação EAD da Faculdade Damásio(2016-2023).

Osmar Fernando Gonçalves Barreto

Pós-doutorando da Faculdade de Direito da Universidade de Coimbra, Portugal (2025 - até o momento). Doutor em Função Social do Direito pela Faculdade Autônoma de Direito de São Paulo - FADISP (2024). Mestre em Direito da Sociedade da Informação pelo Centro Universitário das Faculdades Metropolitanas Unidas - FMU (2017). Bolsista/Pesquisador CAPES (2017). Pós-graduado lato sensu em Direito e Processo do Trabalho pelo Damásio Educacional (2020). Pós-graduado lato sensu em Direito Privado pela Escola Paulista da Magistratura - EPM (2008). Graduado em Direito pelo Centro Universitário das Faculdades Metropolitanas Unidas - FMU (2006). Professor de Direito Individual/Coletivo/Processual/Aplicado do Trabalho e de Estágio de Prática Supervisionada Trabalhista na graduação em Direito do Centro Universitário das Faculdades Metropolitanas Unidas - FMU (2019 - até o momento).

Resumo: A presente pesquisa tem por objetivo específico apontar os aspectos jurídicos que envolvem a utilização de biometria na celebração de Contratos Eletrônicos à luz da Lei nº 13.709, 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), tendo em vista que em seu art. 5º, II, os dados biométricos são considerados dados pessoais sensíveis, de modo que, nas contratações que se derem por meio da formalização via assinatura eletrônica biométrica o agente de tratamento desses dados deverá atender aos requisitos determinados pela LGPD para o tratamento dos dados pessoais sensíveis. Com isso, será suscitado também se a modalidade de assinatura eletrônica biométrica é a mais adequada aos contratantes, tendo em vista que existem diversas modalidades, tais como: click to accept ou opt-in, token, Certificado ICP-Brasil, dentre outras. Através da metodologia da revisão bibliográfica especializada, o presente trabalho tem por objetivo principal esclarecer o que seria biometria, bem como os critérios adequados de utilização deste meio de assinatura eletrônica nos negócios jurídicos eletrônicos, elencando suas características, parâmetros legais, doutrinários e da jurisprudência nacional.

Palavras-chave: contratos eletrônicos; assinaturas eletrônicas; biometria; LGPD; dados pessoais sensíveis.

Abstract: This research aims to highlight the legal aspects involved in the use of biometrics in the execution of Electronic Contracts in light of Law No. 13.709, of August 14, 2018 (General Law on the Protection of Personal Data – LGPD), considering that in its article 5, II, biometric data are considered sensitive personal data, so that contracts formalized through biometric electronic signatures must comply with the requirements established by the LGPD for the

DOI: 10.47573/aya.5379.3.34.19

processing of sensitive personal data. Therefore, it will also be considered whether the biometric electronic signature modality is the most suitable for contracting parties, given that there are several modalities, such as click to accept or opt-in, token, ICP-Brasil Certificate, among others. Through the methodology of specialized bibliographic review, this work aims to clarify what biometrics is, as well as the appropriate criteria for using this means of electronic signature in electronic legal transactions, listing its characteristics, legal parameters, doctrine, and national jurisprudence.

Keywords: electronic contracts; electronic signatures; biometrics; LGPD (Brazilian General Data Protection Law); sensitive personal data.

INTRODUÇÃO

Com a promulgação da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), as pessoas jurídicas e físicas que de alguma forma realizam o tratamento de dados pessoais para o oferecimento de bens e serviços passaram a ter que seguir as determinações da referida lei em suas operações. E com os processos de digitalização de documentos jurídicos e consequentemente com o avanço dos mecanismos de assinatura eletrônica, tem sido cada vez mais comum a utilização da biometria em assinaturas de contratos eletrônicos, o que, segundo a LGPD, são considerados dados pessoais sensíveis (art. 5º, II), sendo que a biometria é considerada uma forma muito segura de aferir que a pessoa que assinou ou contratou determinado bem ou serviço é ela de fato.

Com isso, a metodologia utilizada será hipotético-dedutiva, de modo que se busque explicitar os aspectos jurídicos envolvendo contratações eletrônicas com a formalização por meio da biometria. Desta forma, inicialmente serão tratadas a parte conceitual e a de formalização dos contratos eletrônicos. Posteriormente serão levantados os tipos de biometria capazes de serem utilizados como assinatura eletrônica. E, por fim, analisaremos os aspectos jurídicos e a segurança jurídica atinentes à assinatura eletrônica biométrica.

DOS CONTRATOS ELETRÔNICOS

Conceito de Contratos Eletrônicos

Em primeiro lugar, vamos trazer a conceituação dos contratos tradicionais, aqueles que não são celebrados por meios informatizados, sendo utilizada a conceituação dada por Flávio Tartuce (2023, p. 1):

> O contrato é um ato jurídico bilateral, dependente de pelo menos duas declarações de vontade, cujo objetivo é a criação, a alteração ou até mesmo a extinção de direitos e deveres de conteúdo patrimonial. Os contratos são, em suma, todos os tipos de convenções ou estipulações que possam ser criadas pelo acordo de vontades e por outros fatores acessórios.

Enquanto, na conceituação dos contratos eletrônicos, temos o seguinte:

> O contrato eletrônico deve ser conceituado como o negócio jurídico contratual realizado pela manifestação de vontade das posições jurídicas ativa e passiva, expressa por meio eletrônico no momento de sua formação. Portanto, a manifestação de vontade por meio eletrônico sobrepõe-se à sua instrumentalização, de maneira que não é uma nova categoria contratual, mas sim forma de contratação por manifestação da vontade expressa pelo meio eletrônico (Rebouças 2018, p. 33).

Desta forma, analisando ambos os conceitos, podemos depreender que o contrato existe a partir do momento em que duas ou mais pessoas manifestam sua vontade com o objetivo de criar, alterar ou extinguir algum direito comum entre elas, tendo por diferença apenas a forma como será manifestada a vontade, que, no caso do contrato eletrônico, será por meio de algum ambiente informatizado. Não nos ateremos aos princípios dos contratos nem aos requisitos objetivos, subjetivos e formais de existência, validade e eficácia, porque os mesmos são aplicáveis aos contratos eletrônicos; portanto, não há necessidade de serem tratados nesta pesquisa.[1]

Da Classificação dos Contratos Eletrônicos

Conforme veremos, os contratos eletrônicos se classificam em contratações interpessoais, interativas e intersistêmicas. As contratações eletrônicas interpessoais, segundo Souza (2009, p. 105):

> As partes obrigatoriamente dependerão da utilização dos computadores conectados à Internet para a formação do vínculo contratual, pois as manifestações de vontade ocorrem no mundo virtual e a partir da comunicação estabelecida entre o proponente e o oblato; as partes reúnem-se e interagem em meio virtual.

Com isso, percebemos que as contratações interpessoais necessitam que ambas as partes estejam em tratativas por meio do mundo virtual para que seja concretizado, situação esta que é bem explicada por Rebouças (2018, p. 41):

> As contratações interpessoais são usualmente realizadas por troca de correspondência eletrônica (contrato “entre ausentes”), por meio de chats ou sistemas de mensageria instantânea (contrato “entre presentes”) e atualmente podemos também pensar nas situações envolvendo redes sociais e microblogs (v.g. Twitter) que, dependendo da forma como são utilizados, poderão ser configuradas como contrato “entre presentes” ou “entre ausentes”.

No caso das contratações interativas, que são realizadas de forma massificada quando comparada com os outros meios, segundo Jovanelle (2012, p. 88):

1 A teoria tradicional dos negócios jurídicos; as regras relativas à oferta e à aceitação; o princípio da liberdade das formas (sobretudo!); os princípios contemporâneos da boa-fé, função social e equilíbrio; e, por evidente, a obrigatoriedade aplicam-se aos contratos eletrônicos tal e qual sucede com seus equivalentes mais ortodoxos (Gramstrup, 2018, p.5).

> Normalmente, os contratos interativos são caracterizados pela apresentação de cláusulas unilateralmente preestabelecidas pelo proprietário do website, sem possibilidade de discussão e alteração de tais cláusulas pela contraparte, que deverá aceitá-las em bloco se quiser celebrar o negócio, ou rejeitá-las, também em bloco, abrindo mão da contratação.

Já nas contratações intersistêmicas, ou seja, sem envolvimento humano, mas somente entre computadores previamente programados, temos a seguinte explicação:

> Contratações intersistêmicas – tal forma de contratação ocorre nas hipóteses em que são realizadas operações de compra e venda, por exemplo, de forma automatizada entre um distribuidor e o produtor. Ou seja, são hipóteses em que houve uma prévia programação pelos representantes legais de cada uma das sociedades empresárias ou do próprio consumidor, no sentido de que ao realizar a venda de um produto para a outra parte, ou para o consumidor, o sistema irá automaticamente realizar a baixa de tal produto no estoque e, havendo necessidade, emitirá uma ordem automática de compra junto ao produtor para a reposição dos níveis do estoque (Rebouças, 2018, p. 52).

Até então, a maior parte da doutrina apenas retrata as três classificações que já mencionamos, porém, segundo Rebouças (2018, p. 56), existe, também, a classificação de *Smart Contracts:*

> Os *Smart Contracts* são caracterizados por uma prévia programação de dados, atualmente utilizando linguagens de programação que possam garantir a inviolabilidade por um sistema de criptografia e verificação pública, tal como se dá com o Blockchain, o qual representa uma "tecnologia descentralizada de registro de dados".

Com isso, as partes estipulariam as cláusulas contratuais no próprio sistema, que, ao atingir os elementos esperados, autoexecutaria as obrigações acordadas, podendo ser considerado uma contratação híbrida (interpessoal e intersistêmica).[2]

DA FORMALIZAÇÃO DOS CONTRATOS ELETRÔNICOS

Antes de passarmos para as quatro fases ligadas à formalização dos contratos, na doutrina muito se fala sobre os contratos serem celebrados entre presentes e entre ausentes.

> Se o contrato está na categoria dos firmados entre presentes (onde há simultaneidade nas declarações das partes, como nos contratos realizados em chats – ambientes de conversação –

2 Portanto, acreditamos que o Smart Contract é uma forma de contratação eletrônica mista, sendo o seu primeiro momento formalizado sob a característica de contrato interpessoal e no momento subsequente concluído (execução do contrato) sob a característica de contrato intersistêmico, execução automática e integralmente eletrônica (Ibid., p. 57).

> ou por videoconferência, situações análogas às dos contratos firmados por telefone), tem-se por celebrado no momento em que a aceitação é emitida pelo oblato, ou seja, no momento em que o aceitante concorda com a realização do negócio (Rizzardo, 2023, p. 102).

No caso dos contratos celebrados entre ausentes, existirá um lapso temporal entre a proposta e a aceitação, por exemplo, quando os trâmites realizados pelas partes são por meio de correio eletrônico (e-mail), a parte que deveria manifestar o aceite pode demorar alguns dias, o que tornaria o contrato celebrado entre ausentes.

> Já nos contratos firmados entre ausentes (quando não há simultaneidade nas informações – caso dos contratos enviados por e-mail ou, ainda, nas compras realizadas em websites – páginas eletrônicas – onde existem contratos com cláusulas preestabelecidas e considerados contratos de adesão), o momento da formação é aquele em que o oblato expede a aceitação (Ibid., p. 102).

Fase Pré-contratual

A fase pré-contratual ou preliminar é o momento no qual as partes apresentam suas intenções, negociam e buscam encontrar um denominador comum entre elas que possa determinar a celebração futura de um contrato. Nesta fase, em regra, não há vinculação obrigacional entre as partes, justamente por estarem na fase de conhecimento do negócio jurídico que querem celebrar, porém, conforme muito bem explica Caio Mário da S. Pereira (2015, p. 34), há exceção neste aspecto:

> Pode surgir responsabilidade civil para os que participam das negociações preliminares, não no campo da culpa contratual, porém no da aquiliana [...], somente no caso de um deles induzir o outro à crença de que o contrato será celebrado, levando-o a despesas ou a não contratar com terceiro etc., e depois recuar, causando-lhe dano.

Ou seja, mesmo sem força vinculante, a fase pré-contratual gera responsabilização civil quando ocorrer prejuízo ou dano para a outra parte, ou quando houver a quebra do princípio da boa-fé, como assevera Carlos Roberto Gonçalves (2013, p. 73):

> Embora as negociações preliminares não gerem, por si mesmas, obrigações para qualquer dos participantes, elas fazem surgir, entretanto, deveres jurídicos para os contraentes, decorrentes da incidência do princípio da boa-fé, sendo os principais os deveres de lealdade e correção, de informação, de proteção e cuidado e de sigilo. A violação desses deveres durante o transcurso das negociações é que gera a responsabilidade do contraente, tenha sido ou não celebrado o contrato.

Da Oferta (Proposta)

Após a fase preliminar de negociações, o policitante formula uma proposta para que a outra parte (policitado) possa manifestar sua vontade de celebrar o negócio jurídico. Lembrando que a formulação da proposta gera obrigação de cumprimento por parte de quem a formulou, salvo quando houver situações atinentes ao negócio ou à situação em questão, ou quando a proposta estipular um prazo de validade da mesma[3].

> Para valer, é preciso ser formulada em termos que a aceitação do destinatário baste à conclusão do contrato. Não deve ficar na dependência de nova manifestação da vontade, pois a oferta, condicionada a ulterior declaração do proponente, proposta não é no sentido técnico da palavra. Exige-se que seja inequívoca, precisa e completa, isto é, determinada de tal sorte que, em virtude da aceitação, se possa obter o acordo sobre a totalidade do contrato. Deve conter, portanto, todas as cláusulas essenciais, de modo que o consentimento do oblato implique a formação do contrato (Gomes, 2022, p. 93).

Essas mesmas regras valem tanto para os contratos tradicionais quanto para os eletrônicos, e quando olhamos, também, pelo prisma do Código de Defesa do Consumidor ("CDC"), notamos que o policitante deve cumprir o que está ofertando ao público, sob pena de responsabilização com base nos arts. 35, I e 84, do CDC). O policitante apenas estaria isento se a oferta fosse limitada ao estoque, como muito bem explica Gonçalves:

> A proposta aberta ao público, por meio de exibição de mercadorias em vitrinas, catálogos, anúncios nos diversos meios de divulgação etc., vincula o ofertante. O fornecedor deve assegurar não apenas o preço e as características dos produtos e serviços, mas também as quantidades disponíveis em estoque. Deve, assim, atender à clientela nos limites do estoque informado, sob pena de responsabilidade (Gonçalves, op. cit., p. 80).

A proposta também deixará de obrigar o policitante nas seguintes situações previstas no Código Civil de 2002:

> Art. 428. Deixa de ser obrigatória a proposta:
> I - Se feita sem prazo, a pessoa presente não foi imediatamente aceita. Considera-se também presente a pessoa que contrata por telefone ou por meio de comunicação semelhante;
> II - se, feita sem prazo à pessoa ausente, tiver decorrido tempo suficiente para chegar a resposta ao conhecimento do proponente;
> III - se, feita a pessoa ausente, não tiver sido expedida a resposta dentro do prazo dado;

3 Art. 427. A proposta de contrato obriga o proponente, se o contrário não resultar dos termos dela, da natureza do negócio, ou das circunstâncias do caso.

> IV - se, antes dela, ou simultaneamente, chegar ao conhecimento da outra parte a retratação do proponente (Brasil, 2002).

Da Aceitação

Para que a proposta venha a ser de fato efetivada, deverá ocorrer a convergência de manifestação da vontade entre as partes (de quem emite e de quem aceita). Ocorrendo a aceitação entre presentes, ou seja, quando o policitado manifesta seu aceite de imediato, dá-se por concluído o processo de contratação. Entretanto, quando for entre ausentes, segundo Tartuce, por mais que o Código Civil de 2002 tenha acolhido expressamente, por meio do art. 434, a teoria da expedição, que é quando o policitado ao expedir seu aceite, ainda que não tenha ainda chegado ao policitante, a proposta dar-se-á por aceita, mas o referido diploma legal também acolheu a teoria da recepção, vejamos:

> Entretanto, tal regra comporta exceções, sendo certo que o Código Civil também adota a teoria da agnição, na subteoria da recepção, pela qual o contrato é formado quando a proposta é aceita e recebida pelo proponente (art. 434, incs. I, II e III c/c art. 433 do CC). Essa teoria deve ser aplicada nos seguintes casos:
> a) se antes da aceitação ou com ela chegar ao proponente a retratação do aceitante;
> b) se o proponente se houver comprometido a esperar resposta, hipótese em que as partes convencionaram a aplicação da subteoria da recepção; ou
> c) se a resposta não chegar no prazo convencionado (outra hipótese em que houve convenção entre as partes de aplicação da subteoria da recepção). (Tartuce, 2023, p. 172).

Na visão de Gonçalves, o Código Civil de 2002 justamente por permitir as retratações diante da teoria da expedição, na verdade acabou adotando a teoria da recepção:

> Observa-se que o novo diploma estabeleceu três exceções à regra de que o aperfeiçoamento do contrato se dá com a expedição da resposta. Na realidade, recusando efeito à expedição se tiver havido retratação oportuna, ou se a resposta não chegar ao conhecimento do proponente no prazo, desfigurou ele a teoria da expedição. Ora, se sempre é permitida a retratação antes de a resposta chegar às mãos do proponente, e se, ainda, não se reputa concluído o contrato na hipótese de a resposta não chegar no prazo convencionado, na realidade o referido diploma filiou-se à teoria da recepção, e não à da expedição (Gonçalves, 2013, p. 83 - 84).

De toda forma, podemos notar que o Código Civil de 2002 permite que a aceitação possa ser retratada, de modo que se houver a retratação, deverá ser analisado o caso concreto para determinar se o negócio jurídico foi consumado ou não.

Do Lugar

O Contrato, sendo tradicional ou eletrônico, será considerado celebrado no lugar em que ele foi proposto (art. 435 do Código Civil/2002), e essa regra será aplicável até mesmo nos contratos eletrônicos e quando as partes forem de países diferentes, será considerado o local de residência do proponente (art. 9º, parágrafo 2º da Lei de Introdução às normas do Direito Brasileiro). É importante que as partes, para evitarem maiores problemas quanto à lei aplicável ou ao foro de eleição, venham estipular essas questões na própria proposta ou no contrato que irão celebrar. Isso facilitará até mesmo a análise do negócio jurídico, de acordo, por exemplo, com a legislação que as partes escolheram seguir. "Denota-se que o legislador preferiu a uniformização de critérios, levando em conta o local em que o impulso inicial teve origem. Ressalve-se que, dentro da autonomia da vontade, podem as partes eleger o foro competente (foro de eleição) e a lei aplicável à espécie" (Ibid., p. 84).

BIOMETRIA

Conceito de Biometria

"O termo biometria deriva do grego bios (vida) + metron (medida) e, na autenticação, refere-se à utilização de características próprias de um indivíduo para proceder à sua autenticação e/ou identificação perante um SI de uma organização". (Magalhães; Santos, 2003, p.5) A biometria é bastante utilizada em investigações criminais, visto que é um dos principais meios de identificar uma pessoa de forma mais assertiva. De modo geral, a biometria é definida da seguinte forma:

> A biometric is defined as a unique, measurable, biological characteristic or trait for automatically recognizing or verifying the identity of a human being. Statistically analyzing these biological characteristics has become known as the science of biometrics. These days, biometric technologies are typically used to analyze human characteristics for security purposes. Five of the most common physical biometric patterns analyzed for security purposes are the fingerprint, hand, eye, face, and voice[4] (Soutar *et al.*, 1999, p. 1).

Ou seja, como dito no conceito acima, a biometria demonstra traços biológicos que nos individualizam, de modo que sejamos identificados de forma automática, o que traz segurança tanto nas investigações criminais como, por exemplo, na contratação de algum serviço bancário. O banco sente segurança para lhe conceder

4 Uma biometria é definida como uma característica ou traço biológico exclusivo, mensurável, para reconhecer ou verificar automaticamente a identidade de um ser humano. A análise estatística dessas características biológicas ficou conhecida como a ciência da biometria. Atualmente, as tecnologias biométricas são tipicamente usadas para analisar características humanas para fins de segurança. Cinco dos padrões biométricos físicos mais comuns analisados para fins de segurança são a impressão digital, a mão, o olho, o rosto e a voz. (Tradução livre do autor)

um crédito porque, pela biometria, ficou demonstrado que você é quem diz ser. Veremos diante, por meio de definições breves, temos 5 modalidades de biometria que são muito utilizadas, principalmente nas contratações eletrônicas, sendo elas: reconhecimento facial, geometria da mão, reconhecimento pela íris, reconhecimento pela retina e impressão digital.

Reconhecimento Facial

O reconhecimento facial tem sido um dos métodos mais utilizados, juntamente com a impressão digital, nas contratações eletrônicas. Por exemplo, em serviços bancários você só consegue contratar a abertura de conta, empréstimo pessoal, seguros, cartão de crédito etc., assim como utilizar algumas plataformas de assinatura eletrônica, fornecendo sua biometria facial. Baccarin conceitua esse método da seguinte forma:

> O reconhecimento facial pode ser entendido como uma aplicação de inteligência artificial que se utiliza da técnica de coleta de biometria baseada em traços do rosto humano. Esse processo é realizado a partir da medição de pontos da face que fazem uma ligação algorítmica de traços e tamanhos, levando em consideração a distância exata entre o nariz e orelhas, espaçamento dos olhos, tamanho da testa, contorno dos lábios, entre outras medidas. A partir dessas medições do rosto, extrai-se o dado biométrico, que possibilita a verificação e a autenticação da identidade de uma pessoa ao basear-se nas características exclusivas e específicas desse indivíduo (Baccarin, 2023, p. 36)

Com a explicação acima dada por Baccarin, a inteligência artificial realiza os cálculos matemáticos necessários para determinar as medidas exatas da face humana e para que o reconhecimento facial venha a ser efetivo, "necessita de um banco de dados que contenha imagens para haver um reconhecimento automático" (Amorim *et al.,* 2018, p. 10)

Impressão Digital

A impressão digital é conceituada da seguinte forma por Pinheiro (2008, p. 64):

> A captura da imagem da impressão digital ocorre por meios ópticos, sendo que essa imagem é processada digitalmente pelo sistema, que identifica as características datiloscópicas, comparando com os registros de banco de dados, determinando ou não o acesso (Pinheiro, 2008 *apud* Weber, 2012, p. 55).

Além disso, cada dedo possui um desenho que decorre do formato das suas minúcias; com isso é considerada uma biometria muito segura, porque "esses desenhos possuem configuração aleatória, ou seja, são únicos para cada indivíduo, de acordo com as condições encontradas no processo de desenvolvimento embrionário e genético". (Souza, 2020, p. 85). Carlos Alberto Motta (2008, p. 7),

explica que a impressão digital não pode sofrer mutação para poder resguardar esse método:

> Os desenhos digitais nunca são idênticos em dois indivíduos. É este, aliás, o ponto essencial: porque a imutabilidade do desenho digital em cada pessoa perderia todo o seu interesse prático se dois indivíduos pudessem apresentar desenhos semelhantes. Os gêmeos, quando do mesmo ovo, apresentam desenhos papilares extremamente semelhantes, mas nunca absolutamente iguais. Existem sempre pontos característicos que permitem fazer-se a distinção. A variedade é tão grande que, em milhões de impressões já estudadas e fichadas em todo o mundo, nunca encontraram duas pessoas iguais, são tão variáveis, porém nunca iguais (Motta, 2008 *apud* Weber, op. cit., p. 56).

Esta modalidade tem sido usada em votação nas eleições, desbloqueio de celular e aplicativos, inclusive os bancários, para o registro de ponto eletrônico nas empresas, para o controle de acesso de pessoas em alguns estabelecimentos e para assinatura eletrônica, dentre outras funcionalidades.

Geometria da Mão

Esta biometria é utilizada no registro de ponto do emprego e, também, no controle de acesso de pessoas em ambientes públicos e privados, tendo a seguinte definição:

> A biometria baseada em características da mão fundamenta-se num conjunto de medidas que podem ser extraídas recorrendo a alguns pontos característicos da mão, as cinco pontas dos dedos e os quatro vales entre eles. Um dos grandes obstáculos destes sistemas reside na detecção destes pontos e, dada a dificuldade nessa detecção, muitas das vezes são impostas restrições na fase de aquisição de modo a facilitar a mesma. Estas restrições causam desconforto ao utilizador e limitam a aplicação deste tipo de sistemas. (Amorim *et al.*, 2018, p. 11)

Porém, como muito bem especificado na definição, este tipo biométrico não é muito seguro em razão da dificuldade em registrar de forma individualizada o formato da mão, visto que podem existir semelhantes.

Reconhecimento pela Íris

Atualmente vemos a utilização do reconhecimento pela íris no acesso ao celular e a alguns aplicativos, sendo considerado um dos meios mais seguros de reconhecimento de um indivíduo.

> The iris is an externally visible yet protected organ whose unique epigenetic pattern remains stable throughout adult life. These characteristics make it very attractive for use as a biometric for identifying individuals. Compared with other biometric

> technologies such as face, speech, and finger. Iris recognition can easily be considered as the most reliable form of biometric technology, because the ophthalmologists noted from clinical experience that every iris had a highly detailed and unique texture, which remained unchanged in clinical photographs spanning decades, even medical surgery can't change it.[5] (Ali, E. M.; Ahmed, E. S.; Ali, A. F., 2007, p. 636).

Ou seja, pelo fato de a íris não poder sofrer mutações e danos, ela se torna a mais segura, visto que, além de não permitir adulteração ou plásticas, ela conseguirá definir quem é a pessoa correspondente daquele reconhecimento realizado.

Reconhecimento pela Retina

De acordo com o conceito dado por Pinheiro (2008, p. 70-71), muito bem traduzido por Weber (2012, p . 53), o reconhecimento pela retina:

> É o método de identificação do indivíduo por meio das características dos vasos da retina. O indivíduo precisa olhar fixamente para um ponto de luz de infravermelho para que a imagem dos padrões da veia seja capturada e armazenada em um banco de dados para fins de comparação futura.

Assim como a íris, esse modelo de biometria também é considerado seguro para a identificação, "entretanto, a retina é uma parte do organismo humano que pode sofrer alterações em virtude de algumas anomalias como diabetes, pressão alta, catarata, miopia ou hipermetropia entre outras, afetando o escaneamento da retina" (Costa, 2009, p. 7)

ASSINATURA ELETRÔNICA BIOMÉTRICA À LUZ DA LGPD

Aspectos jurídicos da Assinatura Eletrônica

Com o advento da era da informatização, as assinaturas eletrônicas e digitais passaram a ter maior relevância no mundo jurídico, visto que traz maior eficiência econômica de tempo, papel e custos com correios, podendo a assinatura ocorrer por diversas formas: plataformas de assinatura, via click-to-accept (clique para aceitar) em sites de e-commerce, manifestação de aceite por e-mail e aplicativos de mensageria, dentre outras formas. De acordo com Augusto Tavares Rosa Marcacini, a assinatura eletrônica possui a mesma eficácia de uma assinatura de próprio punho:

5 A íris é um órgão externamente visível, mas protegido, cujo padrão epigenético único permanece estável durante toda a vida adulta. Essas características a tornam muito atraente para o seu uso como biometria para a identificação de indivíduos. Comparado com outras tecnologias biométricas como rosto, fala e dedo. O reconhecimento da íris pode facilmente ser considerado a forma mais confiável de tecnologia biométrica, porque os oftalmologistas observaram, a partir da experiência clínica, que cada íris possui uma textura altamente detalhada e exclusiva, que permanece inalterada em fotografias clínicas ao longo de décadas, e nem mesmo a cirurgia médica poderia mudá-la. (Tradução livre do autor)

> Pode ser considerado como assinatura, tanto na acepção vulgar como jurídica, qualquer meio que possua as mesmas características da assinatura manuscrita, isto é, que seja um sinal identificável, único e exclusivo de uma dada pessoa. Se, até recentemente, a escrita manual era o único meio conhecido de gerar um sinal distintivo único e exclusivo, é evidente que para o Direito não se deixava margem para questionar o que se entendia por 'assinatura'. Na medida em que a evolução da técnica permite uma 'assinatura eletrônica' que possua estas mesmas características, possível se mostra dar-lhe o mesmo significado e eficácia jurídica da assinatura manual (Marcacini, 2002 *apud* Martins, 2016, p. 69)

A assinatura eletrônica ocorre por meio da criptografia simétrica (convencional) ou assimétrica. Na criptografia simétrica, dá-se com o uso de uma chave secreta, por meio de uma senha ou código, no qual o destinatário, ao estar na posse da chave (senha ou código), poderá ler a mensagem ao desencriptá-la (Behrens, 2007, p. 36). Já na criptografia assimétrica, que é a mais atual e mais utilizada, bem como considerada a mais segura por não ser possível usar a mesma chave para desincriptar o documento, segundo Augusto Tavares Rosa Marcacini (1999, p .1):

> A criptografia assimétrica, ao contrário da convencional (que pede a mesma chave tanto para cifrar como para decifrar a mensagem), utiliza duas chaves, geradas pelo computador. Uma das chaves, dizemos ser a chave privada, a ser mantida em sigilo pelo usuário, em seu exclusivo poder, e a outra, a chave pública, que, como sugere o nome, pode e deve ser livremente distribuída. Estas duas chaves são dois números que se relacionam de tal modo que uma desfaz o que a outra faz. Enviando a mensagem com a chave pública, geramos uma mensagem cifrada que não pode ser decifrada com a própria chave pública que a gerou. Só com o uso da chave privada poderemos decifrar a mensagem que foi codificada com a chave pública. E o contrário também é verdadeiro: o que for encriptado com o uso da chave privada só poderá ser decriptado com a chave pública.

Diante desses avanços, o Governo Federal, em 2001, editou a Medida Provisória nº 2.200-2, de 24 de agosto de 2001[6], que instituiu a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, bem como estabeleceu o Comitê Gestor da ICP-Brasil para gerir e credenciar a Autoridade Certificadora Raiz (AC-Raiz), as Autoridades Certificadoras (ACs) e as Autoridades de Registro (ARs). A utilização de certificados digitais ICP-Brasil é considerada a mais segura no mercado, visto que para conseguir essa certificação, a pessoa física ou jurídica passará por um processo rígido de autenticação e atestamento de sua identidade. Tanto é que, ao utilizar um certificado digital no processo de assinatura de algum contrato ou documento, o art.

6 Essa Medida Provisória continua em vigor em razão da mesma ter sido editada antes da publicação da Emenda Constitucional nº 32, de 11 de setembro de 2001, que instituiu o prazo limite de vigência de 60 dias, prorrogável única vez por igual período.

10, § 1º, da MP nº 2.200-2/2001[7], atribuiu a presunção de veracidade perante as partes e terceiros. A referida MP também permite que assinaturas sem certificado digital ICP-Brasil sejam aceitas como válida juridicamente, desde que aceita entre as partes (art. 10, §2º). Em 2020, o Governo Federal promulgou a Lei nº 14.063, de 23 de setembro de 2020, que disciplina o uso de assinaturas eletrônicas entre entes públicos e pessoas jurídicas de direito privado e físicas. Nesta lei, o art. 4º, classifica os tipos de assinaturas eletrônicas a serem utilizados:

> Art. 4º Para efeitos desta Lei, as assinaturas eletrônicas são classificadas em:
> I - assinatura eletrônica simples:
> a) a que permite identificar o seu signatário;
> b) a que anexa ou associa dados a outros dados em formato eletrônico do signatário;
> II - assinatura eletrônica avançada: a que utiliza certificados não emitidos pela ICP-Brasil ou outro meio de comprovação da autoria e da integridade de documentos em forma eletrônica, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento, com as seguintes características:
> a) está associada ao signatário de maneira unívoca;
> b) utiliza dados para a criação de assinatura eletrônica cujo signatário pode, com elevado nível de confiança, operar sob o seu controle exclusivo;
> c) está relacionada aos dados a ela associados de tal modo que qualquer modificação posterior é detectável;
> III - assinatura eletrônica qualificada: a que utiliza certificado digital, nos termos do § 1º do art. 10 da Medida Provisória nº 2.200-2, de 24 de agosto de 2001.
> § 1º Os 3 (três) tipos de assinatura referidos nos incisos I, II e III do caput deste artigo caracterizam o nível de confiança sobre a identidade e a manifestação de vontade de seu titular, e a assinatura eletrônica qualificada é a que possui nível mais elevado de confiabilidade a partir de suas normas, de seus padrões e de seus procedimentos específicos (Brasil, 2020).

Desta forma, podemos ver que existem outras modalidades de assinatura eletrônica que já são aceitas pelo nosso ordenamento jurídico brasileiro, sem a necessidade do uso da biometria. Porém, conforme veremos posteriormente, a biometria tem sido utilizada justamente por conta da segurança maior ao aferir quem de fato assinou.

7 Art. 10, § 1o, da MP. nº 2.200-2. As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei no 3.071, de 1o de janeiro de 1916 - Código Civil.
O art. 131 do Código Civil/1916 passou a ser o art. 219 do Código Civil/2002.

Biometria à Luz da LGPD

Antes de passarmos para a análise do uso da biometria nos contratos eletrônicos (item 4.3), falaremos de forma breve sobre esse dado pessoal sensível, que está no rol exemplificativo do art. 5º, II, da Lei Geral de Proteção de Dados Pessoais "LGPD" (Lei nº 13.709, de 14 de agosto de 2018).

> Art. 5º Para os fins desta Lei, considera-se:
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; (Brasil, 2018)

Como muito bem explicado por Carlos Nelson Konder, os dados sensíveis são aqueles que são passíveis de gerar algum tipo de discriminação, exclusão ou segregação de um determinado indivíduo em razão dos seus dados que foram tratados, atingindo sua dignidade, identidade e privacidade (Konder, 2019, p. 455).

Portanto, por estarem ligados à personalidade da pessoa, os dados biométricos, são dados que, se tratados de forma ilícita, fora da finalidade inicial e de forma mal intencionada, poderão acarretar em prejuízos graves à intimidade e segurança do titular dos dados como discriminações, devendo o agente de tratamento agir de boa-fé e proteger os dados pessoais, que além de ser um direito tutelado pela LGPD é também uma garantia fundamental prevista no art. 5º, LXXIX, da Constituição Federal/1988. Além disso, os agentes de tratamento devem atender aos princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas (art. 6º, I ao X, da LGPD).

Para o uso da biometria na assinatura de contratos eletrônicos, será necessário que o agente de tratamento de dados venha atuar de acordo com as bases legais determinadas pelo art. 11, da LGPD. Ou seja, a assinatura eletrônica com uso da biometria poderia ser utilizada de acordo com a base legal do consentimento (art. 11, I, da LGPD), mediante a autorização específica, destacada e finalidades específicas. E o que mais vem sendo utilizado para permitir o uso da biometria é a base legal da garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos (art. 11, II, alínea "g", da LGPD), conforme muito bem exemplificado por Chiara Spadaccini de Teffé (2022, p . 173-174):

> Instituições bancárias e empregadores podem tratar dados biométricos para a prevenção de fraudes, sem o consentimento dos titulares dos dados, a fim de confirmar que é o empregado autorizado que está entrando em área de acesso restrito da empresa ou que é determinado cliente que está realizando uma transação bancária relevante. Ainda é possível tratar dados sensíveis a partir dessa base legal em um contexto em que se necessite prevenir fraudes em processos de identificação ou de confirmação de identidade por meio de aplicativos utilizados

> em smartphones, como, por exemplo, para a criação de uma conta digital. Da mesma forma, pode-se utilizar essa base para a coleta de dados biométricos de colaboradores para acesso a sistemas financeiros da empresa. Outra situação seria o pedido de atendimento médico-hospitalar, com a utilização de seguro ou de plano de assistência à saúde, que o segurado/beneficiário colocasse seu polegar em um leitor biométrico para confirmar sua identidade, a fim de evitar que outra pessoa utilizasse a cobertura securitária em seu lugar.

Portanto, podemos aferir que o uso da biometria é possível, desde que o agente venha respeitar aos rígidos requisitos da LGPD (inclusive, resguardando os direitos dos titulares, art. 9º, da LGPD), de modo que, para assinatura de contratos eletrônicos a biometria terá como finalidade a prevenção à fraude e à segurança do titular, de modo que garanta que somente ele assinou o contrato (processo de identificação e autenticação), e não um fraudador.

Segurança Jurídica do uso da Biometria nos Contratos Eletrônicos

Antes do início da era da informatização, as assinaturas eram apenas de forma manuscrita, que segundo Pinheiro (2008, p. 78), também é considerada uma forma biométrica (porém, comportamental):

> O reconhecimento da assinatura manuscrita é um método de autenticação pessoal baseado em uma biometria comportamental que analisa a maneira como um indivíduo faz a sua assinatura. Ao assinar, características como a velocidade e a pressão exercida pela mão sobre a caneta e o papel são tão importantes quanto à forma gráfica da assinatura. Esse método biométrico está baseado no fato de que assinar é uma ação de reflexo, não influenciada pelo controle muscular deliberado, com determinadas características (ritmo, toques sucessivos na superfície do papel, velocidade, aceleração) (Pinheiro, 2008 *apud* Weber, 2012, p. 56).

A biometria tem sido usada para a celebração de contratos eletrônicos, visto que a biometria cuida justamente de uma insegurança natural de quem utiliza a assinatura eletrônica que é: será que quem assinou de fato é ela? Essa insegurança diminui consideravelmente quando as plataformas fazem uso da biometria, pelo fato de ela individualizar uma pessoa e não permitir que outra pessoa possua a mesma biometria.

> A biometria por impressão digital é usada para que os envolvidos possam manifestar a sua vontade de contratar por meio da aposição das digitais dos seus dedos em um leitor biométrico. Outros métodos biométricos também poderiam ser utilizados, como, por exemplo, a autenticação facial ou a combinação de duas ou mais formas para minimizar os riscos de fraudes.

> Para afastar qualquer discussão sobre a possibilidade de violação do direito de imagem, o proprietário da característica captada deverá autorizar tal procedimento por meio da aceitação de um termo. Esse termo deverá esclarecer a finalidade da captura, a sua utilização e o seu armazenamento. Após o indivíduo aceitar o termo, declarando que tem ciência e concordância com as informações ali presentes, a captura poderá ser realizada de fato (De Cesaro; Rabello, 2011, p. 54).

Os tribunais já estão proferindo decisões a respeito do uso da biometria na celebração de contratos eletrônicos, vide alguns breves exemplos abaixo.

> APELAÇÃO - INEXIGIBILIDADE DE DÉBITO – EMPRÉSTIMO CONTRATADO POR BIOMETRIA FACIAL VIA APARELHO DE TELEFONIA MÓVEL - DANO MORAL – DANOS MATERIAIS – Pretensão de procedência da demanda – Descabimento – **Hipótese em que ficou comprovada a regular contratação do empréstimo – Utilização de assinatura digital por biometria facial que é lícita** – Desnecessidade de que a assinatura digital seja certificada pelo ICP-Brasil – Contratação do empréstimo que é regular – Inocorrência de dano moral ou de danos materiais – RECURSO DESPROVIDO. APELAÇÃO - LITIGÂNCIA DE MÁ-FÉ – Pretensão de que seja afastada a condenação como litigante de má-fé – Descabimento – Hipótese em que se vislumbra o dolo, a má-fé, na conduta da parte, de modo a identificar um propósito meramente abusivo e caracterizar a litigância de má-fé – RECURSO DESPROVIDO. (TJSP, 2023) – Grifo meu
>
> AÇÃO DE INEXIGIBILIDADE DE DÉBITO C.C. INDENIZAÇÃO POR DANOS MORAIS – Sentença de improcedência – Insurgência da autora – Instituição financeira que comprovou a relação contratual e a existência do débito – **Contratação digital mediante confirmação dos dados pessoais da consumidora e envio de foto do documento pessoal e 'selfie' – Assinatura autenticada por biometria facial – Possibilidade** – Inteligência do art. 3º, da Instrução Normativa INSS Nº 28/2008 – Inexistência de dano moral – Término do contrato que depende da autora, bastando para tanto pedir o cancelamento do cartão e quitar eventuais valores em aberto junto à instituição financeira requerida – Sentença mantida – Honorários majorados com fundamento no art. 85, § 11, do CPC, observada a gratuidade concedida – Recurso improvido, com observação. (TJSP, 2024) – Grifo meu
>
> EMENTA: APELAÇÃO CÍVEL - AÇÃO DECLARATÓRIA DE INEXISTÊNCIA DE DÉBITO C/C INDENIZAÇÃO - EMPRÉSTIMO CONSIGNADO - CONTRATAÇÃO POR VIA ELETRÔNICA - BIOMETRIA FACIAL - VALIDADE. Nas ações em que a parte autora nega a existência do débito, o ônus de provar a legitimidade da cobrança é do réu, pois não é de se exigir daquele a prova negativa de fato. **É válida a contratação**

> **de empréstimo por via eletrônica, mediante autenticação por biometria facial** (TJMG, 2024, grifo meu).
>
> DIREITO DO CONSUMIDOR. AÇÃO DECLARATÓRIA. INEXISTÊNCIA DE RELAÇÃO JURÍDICA. EMPRÉSTIMO CONSIGNADO. ASSINATURA ELETRÔNICA. LEGALIDADE. RECONHECIMENTO POR BIOMETRIA FACIAL. DEPÓSITO DE QUANTIA. VALIDADE E EFICÁCIA DO NEGÓCIO JURÍDICO. SENTENÇA REFORMADA. 1. A validade do negócio jurídico requer agente capaz, objeto lícito, possível, determinado ou determinável e forma esteja prevista ou não vedada em lei, conforme prevê art. 104 do Código Civil. 2. É legal a forma eletrônica de assinatura contratual, ante a Lei n. 13.620/2023, que alterou o § 4º do art. 784 do CPC previu a exequibilidade do título executivo constituído ou atestado por meio eletrônico. 3. **A comprovação de manifestação de aceite do contrato de empréstimo mediante assinatura eletrônica e reconhecimento por biometria facial, aliada à prova de recebimento de quantia constante do ajuste, impõe o reconhecimento de sua validade e eficácia.** 4. Os ônus da sucumbência são invertidos para o autor ser condenado a arcar com as despesas processuais e honorários advocatícios em favor do advogado da parte ré, fixados em 10% sobre o valor da causa, verba cuja exigibilidade ficará suspensa em razão da concessão dos benefícios da gratuidade de justiça em favor do autor, com suporte no art. 98, § 3º, do CPC. 5. Apelo conhecido e provido (TJDFT, 2023, grifo meu).
>
> APELAÇÃO. AÇÃO DECLARATÓRIA DE INEXISTÊNCIA DE DÉBITO C/C REPETIÇÃO DO INDÉBITO E INDENIZAÇÃO POR DANOS MORAIS. CONTRATAÇÃO DE EMPRÉSTIMOS CONSIGNADOS. ASSINATURA ELETRÔNICA POR BIOMETRIA FACIAL. MANIFESTAÇÃO DE VONTADE DA CONTRATANTE. VALIDADE DO NEGÓCIO JURÍDICO. I - **O contrato apresentado em conjunto com os documentos do consumidor, com o consentimento por meio de autorização por reconhecimento facial, e com o comprovante de que a quantia foi depositada na sua conta, com a efetiva utilização dos valores pelo titular, demonstra a validade da contratação.** II - Impugnada a celebração dos contratos, o Banco-réu se desincumbiu de comprovar sua autenticidade, sendo reconhecida, na demanda, a regularidade dos ajustes formalizados digitalmente entre as partes. Mantida a r. sentença. III - Apelação desprovida (TJDFT, 2024, grifo meu).

Desta forma, podemos notar que os tribunais já vêm aceitando a modalidade de assinatura eletrônica por meio do uso de biometria, visto ser um elemento que pode trazer maior facilidade na identificação e evitar questionamentos da outra parte quando alegar que houve fraude ou ato semelhante na celebração de um contrato. O ordenamento jurídico brasileiro recentemente alterou a legislação prevendo que os contratos e documentos assinados eletronicamente terão força executiva

extrajudicial, mesmo que não haja duas testemunhas, bastando que o provedor ou plataforma de assinaturas em que o documento foi assinado ateste a integridade do documento e das assinaturas (art. 784, §4º, do Código de Processo Civil[8], incluído pela Lei nº 14.711, de 2023), ou seja, algumas plataformas já disponibilizam o uso da biometria para realizar uma assinatura eletrônica, de modo que facilitaria da plataforma atestar a autenticidade de quem assinou mediante a análise biométrica. Porém, ainda é necessário ter cautela, visto que ainda será necessário verificar como os tribunais reagirão mediante esta mudança.

CONSIDERAÇÕES FINAIS

Diante de tudo o que foi exposto nesta pesquisa, podemos depreender que o uso da biometria na formalização de contratos eletrônicos não é vedado pela nossa legislação nem pela nossa jurisprudência, que já vem aceitando esta modalidade de autenticação.

Vimos, também, que os dados biométricos, por serem dados sensíveis, além de facilitar a identificação da pessoa que está assinando determinado contrato, evitando possíveis fraudes ou eventuais oposições, requerem cuidados e prevenções para que esses dados não venham a gerar discriminações, segregações e danos ao seu titular durante seu tratamento. Portanto, será necessário que o agente de tratamento dos dados biométricos venha atender a todos os requisitos legais impostos pela Lei Geral de Proteção de Dados Pessoais e outras eventuais leis especiais que possam ser aplicáveis e utilizar a base legal mais adequada ao seu caso, de modo que, não apenas venha se resguardar de uma penalização ou multa, mas, principalmente, resguardar a intimidade, a personalidade, a privacidade e segurança do titular dos dados biométricos, buscando sempre utilizar os meios mais seguros e tecnológicos para proteger esses dados tratados.

REFERÊNCIAS

ALI, E. M.; AHMED, E. S.; ALI, A. F. Recognition of human iris patterns for biometric identification. **JOURNAL OF ENGINEERING AND APPLIED SCIENCE-CAIRO**, v. 54, n. 6, p. 635, 2007. Disponível em: https://www.researchgate.net/profile/Eman-Monir-2/publication/366153509_Recognition_of_Human_Iris_Patterns_for_Biometric_Identification/links/63c5b5cce922c50e999deaa7/Recognition-of-Human-Iris-Patterns-for-Biometric-Identification.pdf - Acesso em: 31 jan. 2026.

AMORIN, Claudio Zurita de. *et al.* **Desenvolvimento de um sistema de identificação e autenticação biométrica: reconhecimento facial.** Universidade Paulista – UNIP, São Paulo, 2018.

8 Art. 784, § 4º. Nos títulos executivos constituídos ou atestados por meio eletrônico, é admitida qualquer modalidade de assinatura eletrônica prevista em lei, dispensada a assinatura de testemunhas quando sua integridade for conferida por provedor de assinatura.

BACCARIN, Cínthia. **Limitações aos sistemas de reconhecimento facial no setor privado: boas práticas em proteção de dados biométricos faciais.** 2023. 154 f. Dissertação (Mestrado em Direito) - Faculdade de Ciências Humanas e Sociais, Universidade Estadual Paulista "Júlio de Mesquita Filho", Franca, 2023. Disponível em: https://repositorio.unesp.br/handle/11449/244748 - Acesso em: 26 jan. 2026.

BEHRENS, Fabiele. **Assinatura Eletrônica e Negócios Jurídicos.** 1. ed. São Paulo: Jaruá, 2006.

BRASIL. **LEI Nº 10.406, DE 10 DE JANEIRO DE 200**2. Brasília/DF. Diário Oficial da União 11.1.2002. Disponível em https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm – Acesso em 18 jan. 2024.

BRASIL. **LEI Nº 8.078, DE 11 DE SETEMBRO DE 1990.** Brasília/DF. Diário Oficial da União 12.9.1990. Disponível em https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm – Acesso em 18 jan. 2026.

BRASIL. **DECRETO-LEI Nº 4.657, DE 4 DE SETEMBRO DE 1942**. Brasília/DF. Diário Oficial da União 9.9.1942. Disponível em https://www.planalto.gov.br/ccivil_03/decreto-lei/del4657compilado.htm – Acesso em 20 jan. 2026..

BRASIL. **MEDIDA PROVISÓRIA Nº 2.200-2, DE 24 DE AGOSTO DE 2001**. Brasília/DF. Diário Oficial da União 27.8.2001. Disponível em: https://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm - Acesso em 03 fev. 2026.

BRASIL. **LEI Nº 13.105, DE 16 DE MARÇO DE 2015.** Brasília/DF. Diário Oficial da União 17.3.2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm - Acesso em 03 fev. 2026.

BRASIL. **LEI Nº 13.709, DE 14 DE AGOSTO DE 2018.** Brasília/DF. Diário Oficial da União 15.8.2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm - Acesso em 05 fev. 2026.

BRASIL. **CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988**. Brasília/DF. Diário Oficial da União 5.10.1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm - Acesso em 05 fev. 2026.

BRASIL. TJSP – Tribunal de Justiça do Estado de São Paulo. **Apelação Cível 1004252-89.2022.8.26.0541.** Relator (a): Ana de Lourdes Coutinho Silva da Fonseca; Órgão Julgador: 13ª Câmara de Direito Privado; Foro de Santa Fé do Sul - 3ª Vara; Data do Julgamento: 17/07/2023; Data de Registro: 17/07/2023.

BRASIL. TJSP – **Tribunal de Justiça do Estado de São Paulo; Apelação Cível 1089597-51.2023.8.26.0100.** Relator (a): Lígia Araújo Bisogni; Órgão Julgador: 23ª Câmara de Direito Privado; Foro Central Cível - 40ª Vara Cível; Data do Julgamento: 18/03/2024; Data de Registro: 18/03/2024.

BRASIL. TJMG – Tribunal de Justiça do Estado de Minas Gerais. **Apelação Cível 1.0000.23.108987-1/001.** Relator(a): Des.(a) Marcelo Pereira da Silva,

11ª CÂMARA CÍVEL, julgamento em 31/01/2024, publicação da súmula em 31/01/2024.

BRASIL. TJDFT – Tribunal de Justiça do Distrito Federal e dos Territórios. **Acórdão 1775831, 07064780220238070003.** Relator: Roberto Freitas Filho, 3ª Turma Cível, data de julgamento: 19/10/2023, publicado no DJE: 10/11/2023.

BRASIL. TJDFT – Tribunal de Justiça do Distrito Federal e dos Territórios. **Acórdão 1816276, 07022715120238070005,** Relator: VERA ANDRIGHI, 6ª Turma Cível, data de julgamento: 15/2/2024, publicado no DJE: 1/3/2024.

COSTA, Ronaldo Martins da. **Uma nova abordagem para reconhecimento biométrico baseado em características dinâmicas da íris humana.** Orientador Prof. Dr. Adilson Gonzaga. Tese (Doutorado – Programa de Pós-Graduação em Engenharia Elétrica) – Escola de Engenharia de São Carlos da Universidade de São Paulo, São Carlos, 2009.

DE CESARO, T. D. C. J.; RABELLO, R. dos S. Um modelo para a implementação de contratos eletrônicos válidos. **Revista Brasileira de Computação Aplicada,** [S. l.], v. 4, n. 1, p. 48-60, dez/2011. DOI: 10.5335/rbca.2013.2061. Disponível em: https://seer.upf.br/index.php/rbca/article/view/2061 - Acesso em: 3 fev. 2026.

GOMES, Orlando. Contratos. **Atualizadores Edvaldo Brito [e coordenador], Reginalda Paranhos de Brito.** 28. ed. – Rio de Janeiro: Forense, 2022. E-book. ISBN 9786559645640. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559645640/ - Acesso em: 18 jan. 2026.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro**, Volume 3: Contratos e Atos Unilaterais. 10. ed. São Paulo: Saraiva, 2013.

GRAMSTRUP, Erik Frederico. Contratos Eletrônicos: Formação, Consentimento, Lei e Jurisdição Aplicável. **Revista de Direito Recuperacional e Empresa. Revista dos Tribunais.** Vol. 8/2018. Abr .– Jun/2018.

JOVANELLE, Valquíria de Jesus. **Aspectos jurídicos dos contratos eletrônicos.** 2012. 133 páginas. Dissertação de Mestrado em Direito Comercial – Faculdade de Direito, Universidade de São Paulo – São Paulo. 2012. Disponível em: https://doi.org/10.11606/D.2.2012.tde-30102012-094950 - Acesso em: 16 mar. 2026.

KONDER, Carlos Nelson. **O tratamento de dados sensíveis à luz da Lei 13.709/2018.** Em: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 1ª ed. – São Paulo: Thomson Reuters Brasil, 2019.

Magalhães, Paulo Sérgio Tenreiro; Santos, Henrique Dinis dos. **Biometria e autenticação.** Conferência da Associação Portuguesa de Sistemas De Informação, 4, Porto, 2003 - " CAPSI 2003: actas" [CD-ROM]. [S.l. : APSI, 2002]. ISBN 972-9354-42-1. Disponível em: https://repositorium.sdum.uminho.pt/handle/1822/2184 - Acesso em: 29 jan 2026

MARTINS, Guilherme M. **Contratos Eletrônicos de Consumo, 3ª edição.** São Paulo: Atlas, 2016. E-book. ISBN 9788597008944. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788597008944/ - Acesso em: 03 fev. 2026.

REBOUÇAS, Rodrigo Fernandes. **Contratos Eletrônicos: Formação e Validade - Aplicações Práticas.** 2. ed. rev. e ampl. - São Paulo: Almedina, 2018.

RIZZARDO, Arnaldo. Contratos. 21ª edição - Rio de Janeiro: Forense/Grupo Gen, 2023. E-book. ISBN 9786559648153. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559648153/ - Acesso em: 17 mar. 2026

SOUTAR, Colin, *et al.* **Biometric Encryption.** ICSA Guide to Cryptography. Vol. 22. New York: McGraw-Hill, 1999. Disponível em: https://www.cse.lehigh.edu/prr/Biometrics/Archive/Papers/BiometricEncryption.pdf - Acesso em: 26 jan. 2026.

Souza, Marco Antônio de. A biometria e suas aplicações. **Revista brasileira de ciências policiais**, v. 11, n. 2, p. 79-102, mai./ago. 2020. Disponível em: http://dspace.mj.gov.br/handle/1/7826 - Acesso em: 30 jan. 2026.

SOUZA, Vinicius Roberto Prioli. **Contratos Eletrônicos e Validade da Assinatura Digital.** 1. ed. - São Paulo: Jaruá, 2009.

TARTUCE, Flávio. **Direito Civil: Teoria Geral dos Contratos e Contratos em Espécie**. v. 3. 18ª edição - Rio de Janeiro: Forense/Grupo GEN, 2023. E-book. ISBN 9786559646913. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559646913/ - Acesso em: 16 mar. 2026.

TEFFÉ, Chiara Spadaccini de. **Dados pessoais sensíveis: qualificação, tratamento e boas práticas**. Indaiatuba/SP: Editora Foco, 2022.

WEBER, Sandra Paula Tomazi. **A utilização da assinatura eletrônica biométrica na formação dos contratos.** 2012. Monografia de Especialização (Especialização em Direito Contratual) - Faculdade de Direito da Pontifícia Universidade Católica de São Paulo, São Paulo, 2012. Disponível em: https://repositorio.pucsp.br/jspui/handle/30038 - Acesso em: 30 jan. 2026.