



centro universitário
unifacvest

**Contratos, documentos e
assinaturas eletrônicas**

Introdução ao Direito digital

Louise Heine

OBJETIVOS DE APRENDIZAGEM

- > Conceituar algoritmos, dados, inteligência artificial, *big data* e *blockchain*.
- > Definir direito ao esquecimento e a posição do Supremo Tribunal Federal sobre o tema.
- > Reconhecer o papel do compartilhamento internacional de dados e da respectiva cooperação entre países.

Introdução

Há quem sustente que, atualmente, vivemos a Quarta Revolução Industrial, cuja pedra fundamental seria a inovação tecnológica. Como toda transformação disruptiva da sociedade, esta não pode ser ignorada pelas ciências jurídicas: é preciso entender como o Direito se relaciona com as inovações que vêm impactando a sociedade de uma forma geral, alterando, de maneira profunda, a vida humana, o Estado, a regulação e os direitos. Nesse contexto, o Direito Digital surge como um meio de adequar a realidade judicial e legislativa a essa nova realidade, sem abandonar princípios essenciais, como o da segurança jurídica.

Como a Era Digital avança em um ritmo mais rápido do que o ordenamento jurídico, surgem lacunas legais, que não abarcam os comportamentos e as relações oriundas da tecnologia. Até que o Estado se adapte, criando regras, a regulamentação existente e novas dinâmicas tendem a encontrar solução no Poder Judiciário. Diante da ausência de legislação específica, não é raro que o Poder Judiciário, sendo provocado, termine por legislar por meio de uma decisão.

No campo do Direito, portanto, as mudanças na sociedade, incluindo a nova realidade digital, devem ser analisadas para que as normas tradicionais possam sofrer as adaptações necessárias. Do mesmo modo, outras normas estão surgindo, diretamente relacionadas com o Direito Digital, e por isso é fundamental conhecer seus principais conceitos, desdobramentos e impactos na vida das pessoas, assunto do qual trataremos neste capítulo. Além disso, definiremos direito ao esquecimento, com destaque para o atual posicionamento do Supremo Tribunal Federal (STF) sobre o tema, e explicaremos o papel do compartilhamento internacional de dados.

Conceitos fundamentais

Antes de mais nada, tratando-se de tecnologia da informação, é preciso definir alguns termos essenciais para entender como funcionam os sistemas e as máquinas. Para o Direito, essa conceituação é indispensável, pois os regramentos e as decisões judiciais deverão levar em consideração o significado de cada termo e a que se refere.

Algoritmos

Os algoritmos são imprescindíveis para os sistemas digitais. Embora hoje sejam amplamente empregados na informática, o conceito surgiu de aplicações matemáticas. *Grosso modo*, caracterizam-se por conter, obrigatoriamente, uma norma estabelecida para um procedimento que, quando empregada, produzirá um resultado, passando por algumas etapas. Assim, os algoritmos formam uma sequência de atos lógicos, raciocínios, instruções, operações, todos ordenados para alcançar um objetivo, de modo que todas as etapas devem ser seguidas.

O algoritmo deve sempre ter claros seu objetivo e a finalidade para a qual se destina. Assim, quando as informações são fornecidas, o processamento delas segue um padrão de tratamento para fornecer um resultado. Com base nisso, é possível perceber que o algoritmo tem uma entrada (*input*) e uma saída (*output*) de informações, a exemplo das instruções do que e de como algo deve ser feito. Segundo Frazão (2018), os algoritmos têm sido utilizados para respostas de questões objetivas e, ainda, para decidir sobre questões subjetivas, complexas e que envolvem juízos sofisticados de valor, como estas: Quem deve ser contratado para trabalhar em uma empresa? Que contrato deve ser celebrado e em quais bases? Qual é a probabilidade de reincidência de determinado criminoso?

É pelo uso dos algoritmos que as máquinas conseguem aprender. Conforme vai recebendo mais informações, o algoritmo vai ficando mais complexo, mais especializado e mais capaz de englobar múltiplas situações. Assim, trabalha com códigos variáveis e comandos de repetição. Uma sequência de algoritmos pode formar um programa de computador ou a funcionalidade de um aplicativo.



Fique atento

Os algoritmos impactam a forma como enxergamos o mundo, atuando sobre o comportamento humano ao influenciarem as escolhas. Segundo Hoffman-Riem (2019), muitas atividades cotidianas, sobretudo nosso consumo midiático, são influenciadas, de forma implícita, pelos algoritmos. Os algoritmos, para o autor, podem ser capazes de observar o comportamento humano, identificando os interesses com o intuito de prever necessidades e atitudes futuras. A isso, chamamos de **capacidade preditiva**.

O fato de os algoritmos terem a capacidade de ampliar seu espectro de atuação por meio dos dados que recebem não significa dizer que não falham. Podem ocorrer comportamentos imprevisíveis ou não éticos, com a discriminação algorítmica, como resultado da programação que foi feita. A discriminação algorítmica nem sempre acontece por um ato intencional. Ela consiste em categorizar pessoas por alguma característica identificada pela programação dos algoritmos e que pode não ser verdadeira.

Dados

Os dados, em um conceito adequado à realidade digital, são as informações coletadas, inseridas e fornecidas para determinada finalidade. Atualmente, essas informações são valiosas e circulam mundialmente. São os dados que abastecem os algoritmos, de modo que a inclusão daqueles nos sistemas são os *inputs*, que receberão tratamento para chegar a uma resposta: o *output*.

Os dados são o principal ativo de boa parte das organizações e movem a economia digital, de modo que protegê-los de forma consistente é fundamental para a preservação do Estado Democrático de Direito e das liberdades públicas. Portanto, proteger os dados é uma forma de proteger os cidadãos e a sociedade. No Brasil, o Marco Civil Regulatório da Internet (Lei nº 12.965, de 23 de abril de 2014) e a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018 [LGPD]) trazem previsões legais sobre como os dados devem ser tratados, direitos e obrigações das pessoas físicas e

jurídicas, consequências do descumprimento, obrigações e deveres do Poder Público, entre outras.

A LGPD brasileira foi inspirada na legislação da União Europeia, a GDPR (“General Data Protection Regulation”). Basicamente, a GDPR objetiva proteger o titular do dado pessoal, obrigando os serviços de coleta de dados a informar claramente que o fazem. No Brasil, o foco da LGPD também é a proteção de dados pessoais da pessoa natural, sejam eles sensíveis ou não. Nas palavras de Haikal e Pinheiro (2013), a proteção dos dados pessoais tem, como premissa, a defesa da privacidade. Com a privacidade assegurada de maneira apropriada, as liberdades individuais estarão protegidas.



Fique atento

É importante esclarecer que a lei brasileira prevê as obrigações para quem detém os dados pessoais dos usuários em qualquer meio, estejam eles conectados ou não à internet, sejam físicos ou digitais. Além disso, é clara ao determinar que os dados pessoais a serem protegidos se referem à pessoa identificada ou identificável, ou seja, havendo, no cadastro, qualquer meio de determinar a identidade do usuário.

Inteligência artificial

Inteligência artificial é uma tecnologia utilizada por sistemas, máquinas e computadores que simulam o pensamento humano para a tomada de decisões, o aprendizado e a execução de tarefas, no intuito de prever comportamentos e resultados, entre várias outras aplicabilidades, de forma autônoma. A inteligência artificial, então, abastecida com dados, funciona com a utilização de algoritmos, produzindo previsões. Algumas das decisões automatizadas, quando se referem a um indivíduo, são baseadas em métodos para a análise de grande volume de dados. Essas informações podem resultar em riscos ou ofensas aos direitos individuais, como autonomia, igualdade e personalidade.

Lyon (2003) refere que a sociedade, hoje, caracteriza-se pelas relações remotas, de modo que os dados pessoais se transformaram em uma forma de representação das pessoas, sendo determinantes para abrir ou fechar as portas de oportunidades e acessos. Nesse sentido, Doneda *et al.* (2018) atentam para o fato de que as decisões automatizadas também têm potencial para violar os direitos fundamentais, o que pode ser minimizado pelo cumprimento de determinados parâmetros éticos e legais que assegurem a transparência a respeito do uso das informações, bem como a correção e atualização das informações que servem como *input* do algoritmo.



Fique atento

A inteligência artificial permite, à máquina, aprender, em um processo chamado de **machine learning**. A partir do abastecimento com dados, seguindo os passos do algoritmo e treinos, a máquina é capaz de aprender, ampliar sua atividade e fornecer respostas às questões. Outro termo importante é **deep learning**, que consiste na maneira de estruturação da inteligência artificial inspirada no funcionamento das redes neurais dos animais. Os circuitos de programação do algoritmo são feitos em camadas, variando a complexidade, os tipos de dados e o modo de tratamento para gerar a resposta.

Big data

Muito se ouve falar sobre *big data*, uma das palavras do momento quando o assunto é tecnologia. O termo é utilizado para remeter a uma grande quantidade de dados, um conjunto que expressa uma coleção imensa de tipos de dados com qualidade diversificada, com fontes variadas e enorme capacidade de processamento rápido. Seu uso serve para diversos fins, tanto para entes privados quanto públicos. Segundo Hoffmann-Riem (2019), os dados não são coletados, acumulados, analisados e utilizados apenas no âmbito da economia privada, mas, também, em âmbito estatal. Porém, os dados pessoais também integram o *big data*, então a preocupação da LGPD é extensiva a ele.



Fique atento

Hoffmann-Riem (2019) afirma que o significado de algoritmos para a seleção e o controle de comportamentos é impulsionado pela disponibilidade do *big data*, que, por sua vez, é uma consequência da algoritmização.

Conforme Laney (2001), são três as características do *big data*: volume, variedade e velocidade. Uma das possibilidades de utilização do *big data* é por meio da inteligência artificial, pois são empregados diferentes procedimentos analíticos para cada diferente finalidade, que é definida conforme o algoritmo programado. A inteligência artificial, então, é capaz de acessar informações do *big data* e processar para uma finalidade, conforme a programação do algoritmo.

Blockchain

No ano de 2018, o Superior Tribunal de Justiça (STJ) analisou um caso considerado paradigma envolvendo instituição financeira. No voto, ao se manifestar, a Ministra Nancy Andrighi definiu que *blockchain* é um tipo de tecnologia que não depende de organização centralizada de dados para intermediar o armazenamento de dados e as operações digitais. Nas palavras de Porto, Lima Júnior e Silva (2019, p. 12), *blockchain* “[...] corresponde à base de armazenamento e registro de dados integralmente digital, na qual podem ser realizados negócios e operações financeiras por meio da codificação computacional”.

Silva e Sousa (2019) mencionam que essa ferramenta foi desenvolvida para servir às áreas financeiras e empresariais, promovendo garantias, como a segurança jurídica, para os *smart contracts*. Funciona, portanto, como blocos de informações e transações regidos por um código, autoexecutável, que permite a execução de contratos e negociações. De fato, o *blockchain* foi criado para servir como suporte para a criação do Bitcoin, uma criptomoeda. É como se fosse um livro-registro cujos dados podem ser acessados por todos, permitindo a transação de valores sem uma instituição financeira como intermediária. Essa cadeia de dados é armazenada e reunida em blocos com uma função *hash*, que Narayanan *et al.* (2016) definem como a característica de imutabilidade, uma vez que os dados são armazenados e submetidos a uma função e, depois disso, não podem ser alterados.

Aqueles que utilizam a tecnologia do *blockchain* desempenham um papel importante, visto que podem monitorar o cumprimento e a execução dos termos codificados, mantendo o anonimato, o que fortalece a noção de segurança do sistema. O uso dessa tecnologia, assim, como enfatiza Lafarre e Elst (2018 *apud* PORTO; LIMA JÚNIOR; SILVA, 2019, p. 14), torna possível que haja a “[...] transparência e a confiabilidade das informações reunidas na rede sem a necessidade de uma instituição centralizadora para outorgar autorização e assumir a responsabilidade pela verificação da veracidade dos dados inseridos e das transações efetuadas”. Porto, Lima Júnior e Silva (2019) comentam que essa tecnologia tem vastas possibilidades de aplicações, além da criptomoeda, como o registro de propriedades, comprovações de autoria e propriedade intelectual, contratos automatizados, remessas internacionais de valores, emissão de títulos privados, organizações descentralizadas autônomas, etc. O Governo do Brasil, por exemplo, utiliza essa tecnologia para autenticar documentos.

Cidadania digital

Falar em cidadania é falar no exercício de direitos por parte dos indivíduos. Em uma sociedade, todos os indivíduos que têm direitos também têm deveres. Assim, surgem as noções de obrigações e responsabilidades. Quando se transporta isso para a área do Direito Digital, entendendo o indivíduo como um cidadão digital, na medida em que consome dados, fornece dados e tem acesso a eles o tempo todo por meio de informações, percebe-se o quão necessária é a observância aos princípios da privacidade, da intimidade e da liberdade de expressão. Todos esses direitos, como fundamentais, são capazes de limitar o outro quando extrapola, no caso concreto, seu bom uso, causando dano moral ou patrimonial. Surge, daí, o dever de indenizar.

A cidadania digital é conectada com a noção da ética e das boas práticas no ambiente digital. Com o crescente aumento das redes sociais, todos os indivíduos têm a possibilidade de se expressar, de opinar e de se manifestar sobre algum assunto. É o pleno exercício da liberdade de expressão. Todavia, não deve servir de justificativa para constranger o outro. A ética e a boa-fé objetiva devem prevalecer tanto nas relações pessoais quanto nas relações virtuais.

Outro aspecto a se considerar é a solução de conflitos pelos meios digitais. Isso ocorre tanto pelo acesso ao Poder Judiciário pelos meios digitais quanto por mediações e negociações feitas pela internet. Já existem, inclusive, serviços de mediação de conflitos por meio da internet. Seja qual for o meio, as pessoas cada vez mais estão praticando atos da vida cotidiana pela internet. Na esfera pública, os órgãos administrativos já divulgam, no ambiente virtual, seu portal da transparência, empresas privadas divulgam seus balancetes anuais, é possível declarar o imposto de renda pela internet, as notas fiscais já são eletrônicas, há serviços relativos à Previdência Social que apenas são prestados por meios digitais, etc. Enfim, há uma vasta utilização dos meios digitais pelas pessoas, de modo que dados pessoais são fornecidos a todo momento.

Para Doneda (2011), é fundamental que se reconheça a necessidade de proteção de dados como um direito autônomo e fundamental para a proteção da personalidade em prol das garantias constitucionais de igualdade, liberdade e dignidade da pessoa humana, proteção da intimidade e da vida privada. A cidadania digital é uma realidade e uma necessidade para otimizar a vida das pessoas e informar, de maneira transparente, dados do Poder Público, além de uma ferramenta de acesso a serviços e informações. Por meio de senhas e assinaturas digitais, é possível transitar, virtualmente,

pelos mais diversos setores, praticando os mais variados atos. Porém, não se deve esquecer de que, para que isso aconteça, dados pessoais são inseridos e circulam nesse ambiente. Nesse sentido, medidas protetivas sobre o tratamento e a finalidade desses dados devem ser cumpridas por todos, sejam entes privados ou públicos.



Fique atento

Você já ouviu falar do termo **fintech**? As *fintechs* são *startups* que usam a tecnologia aplicada ao mercado financeiro. Seus objetivos incluem aumentar a agilidade das transações financeiras e de investimentos, de forma segura, prática e totalmente digital.

O direito ao esquecimento no Brasil

O direito ao esquecimento vem sendo discutido há algum tempo no Brasil. Em países da União Europeia, ele é reconhecido pelas Cortes desde 2014. Em decisão proferida sobre esse direito, foi decidido que o Google deveria, por si, avaliar cada pedido de retirada de notícias ou de informações sobre alguém, mediante requerimento, analisando se o conteúdo ofende algum direito do requerente ou se há um interesse público na manutenção da informação. Esse direito, portanto, consiste na possibilidade de requerer, judicialmente, a exclusão de um fato ocorrido no passado, de dados, notícias e qualquer divulgação em meio digital que cause dor ou constrangimento a uma pessoa. O exercício desse direito não tem relação com a veracidade ou não dos fatos, de modo que é possível pedir o esquecimento de quaisquer fatos, verdadeiros ou não.



Fique atento

Na internet, as informações circulam de maneira muito rápida. Os motores de busca são capazes de identificar pessoas e apresentar notícias bastante antigas, de forma que é possível levantar a história pregressa de qualquer pessoa. Algumas informações, porém, podem estar desatualizadas, enquanto outras podem não ser apresentadas dentro do contexto. O que se deve ter em mente é que o direito ao esquecimento tem relação com a reputação, a honra, a privacidade e possíveis sentimentos negativos que a divulgação daquela informação pode fazer emergir. Em oposição a esse direito, estão o direito à informação e o conhecimento considerado de interesse público.

O direito ao esquecimento, por ter como motor motivador um fator subjetivo, é um direito personalíssimo. A Lei nº 12.965/2014, conhecida como “Marco Civil Regulatório da Internet”, prevê a possibilidade de requerer a exclusão de informações sobre o usuário por ofensa a algum direito Brasil (2014). Essa exclusão, porém, refere à retirada de conteúdos considerados ilícitos, postados por terceiros, e deverá ser julgada por juízes de direito, afastando, dos provedores de internet, a discricionariedade pela retirada da informação. O Poder Judiciário deverá pesar, no caso, o direito à liberdade de expressão e à informação em oposição ao direito de privacidade. Não deixa de ser, então, um embate entre direitos fundamentais. Moreira (2016) aponta que o um não anula o outro, mas eles impõem, ao intérprete, a composição dos conflitos de interesses para determinar os limites concretos aos princípios em choque.

A existência do direito ao esquecimento foi reconhecida e aplicada no Brasil antes do surgimento de uma legislação específica, por meio do Enunciado 531 (aprovado durante a VI Jornada de Direito Civil, em 2013), o qual prevê que “A tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento” (BRASIL, [2013], documento *on-line*). Atualmente, no Brasil, além de na Constituição Federal, o direito ao esquecimento encontra respaldo legal no Marco Civil da Internet, no Código de Defesa do Consumidor, na Lei de Cadastro Positivo, na Lei de Acesso à Informação e na LGPD. Moreira (2016) afirma que, nesse contexto, a LGPD desponta como um novo e importante arsenal para contribuir com a efetividade da proteção aos direitos da personalidade garantidos na Carta Magna.

O direito ao esquecimento como um direito fundamental associado à dignidade da pessoa humana e à inviolabilidade pessoal, ao encontro do que preveem os arts. 1º, III, e 5º, X, da Constituição Federal (BRASIL, [2020a]). Esse direito, em que pese não seja considerado como fundamental pelo ordenamento jurídico, tem vínculo íntimo com cláusulas péticas. Os autores justificam essa posição pela observação do que ocorre no Direito Penal, quando um indivíduo que passa por um processo, tendo ou não condenação, não deve ter seu registro informacional permanente usado contra ele para evitar que ocorra uma condenação *perene* por fatos do passado.

Para Sarlet (2015), é possível existir um direito fundamental implícito, como seria o caso do direito ao esquecimento. Em outros termos, esse reconhecimento na categoria de direito fundamental pode ser deduzido de direitos expressos, como, por exemplo, os direitos da personalidade. Segundo o autor, na cláusula geral de proteção e promoção da personalidade,

é possível contemplar a proteção que levaria ao reconhecimento do direito ao esquecimento como um direito fundamental.

Nesse contexto, importa mencionar que os ministros do STJ já reconheceram o direito ao esquecimento com fundamento nos direitos de personalidade. Seria, por isso, um direito considerado privado, com forte componente subjetivo. Quando há casos de conflitos entre direitos fundamentais, eles devem ser resolvidos utilizando o sopesamento ou o balanceamento para atingir um equilíbrio.

O entendimento do Supremo Tribunal Federal

No Brasil, já foram julgados alguns casos de direito ao esquecimento. Alguns reconhecidos, outros não. Em fevereiro de 2021, o STF (2021, documento *on-line*), julgando caso que considerou de repercussão geral, firmou o seguinte entendimento:

É incompatível com a Constituição Federal a ideia de um direito ao esquecimento, assim entendido como o poder de obstar, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos e lícitamente obtidos e publicados em meios de comunicação social — analógicos ou digitais. Eventuais excessos ou abusos no exercício da liberdade de expressão e de informação devem ser analisados caso a caso, a partir dos parâmetros constitucionais, especialmente os relativos à proteção da honra, da imagem, da privacidade e da personalidade em geral, e as expressas e específicas previsões legais nos âmbitos penal e cível.

Por maioria dos votos, foi negado provimento ao Recurso Extraordinário 1010606, Brasil (2016), com repercussão geral reconhecida, do famoso caso Aída Curi, vítima de um homicídio célebre nos anos 1950, ocorrido em Copacabana, no Rio de Janeiro. Os familiares da vítima solicitaram o direito ao esquecimento, alegando grande sofrimento com a divulgação e a veiculação de uma reconstituição do caso, que foi ao ar em 2004, no programa “Linha Direta”, da TV Globo, sem sua autorização. Nesse conflito de direitos, foi argumentado que o caso era considerado de domínio e interesse públicos, fazendo parte da história da cidade e sendo, assim, de conhecimento geral. A exibição do episódio em rede nacional e a veiculação pela internet, no entendimento dos Ministros, não deveria ser excluída, pois ofenderia a liberdade de expressão e o direito à informação.

Tal decisão do STF pode ser entendida como na contramão das tendências mundiais. Isso porque, no mundo atual do fluxo de informações, há uma tendência cada vez maior à proteção de dados e informações individuais. Ainda que haja muito espaço para discussões sobre os direitos envolvidos, pela fixação da tese acima, a tendência é que o posicionamento do STF seja adotado pelo Judiciário brasileiro nos demais casos que versarem sobre o tema.



Saiba mais

Em 1958, Aída Jacob Curi foi vítima de violência seguida de morte pelas mãos de três jovens, que, por fim, a atiraram do alto de um edifício na Av. Atlântica, em Copacabana, no Rio de Janeiro. Ronaldo Guilherme de Souza, o principal dos acusados, foi submetido a três julgamentos, tendo sido condenado à pena de oito anos e nove meses de reclusão por homicídio e tentativa de estupro.

O compartilhamento internacional de dados e a cooperação entre países

A LGPD trouxe uma nova perspectiva sobre o compartilhamento de dados entre países. Nos termos da Lei, o titular dos dados é a pessoa natural identificada ou identificável por eles (BRASIL, [2020b]). Os dados e, por consequência, a pessoa merecem proteção, uma vez que a circulação de informações nos meios digitais nem sempre consegue dar segurança sobre a destinação e o tratamento dos dados.

A Lei também faz uma distinção sobre os dados considerados sensíveis, que são aqueles que carregam informações 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, [2020b], documento *on-line*). Todos esses dados, sensíveis ou não, merecem proteção e são objeto da Lei, ainda que a coleta não tenha sido feita de maneira *on-line*. Isso amplia o leque de proteção, incluindo qualquer cadastramento em meio físico do titular dos dados que serão tratados. Por “tratamento de dados”, a Lei estabelece que é todo e qualquer tipo de manipulação realizada com informações pessoais, seja a coleta, a reprodução, o acesso, o armazenamento ou a distribuição. O titular tem o direito a receber todas essas informações de quem coleta os dados, podendo, ainda, solicitar sua exclusão da base de dados ou a correção de dados incompletos ou errados.

Sobre o tratamento de dados pessoais de crianças e adolescentes, refere o art. 14, Brasil ([2020b], documento *on-line*):

Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

§ 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.

§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.

§ 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

§ 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.

§ 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Daí se tira que a legislação teve especial cuidado ao tutelar os dados de menores, observando as disposições do Estatuto da Criança e do Adolescente. Nota-se que os dados pessoais, sendo de menores ou não, observam a exigência de um consentimento do titular ou pessoa responsável. Essas exigências são impostas tanto ao Poder Público quanto às pessoas de direito privado. A exceção, porém, é que o Poder Público pode tratar dados pessoais sem pedir o consentimento do titular sempre que for necessário para a execução de políticas públicas. Além disso, pela LGPD ([2020b], documento *on-line*), poderá tratá-los de maneira diferente em casos excepcionais, como nos casos de:

[...] segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais, que serão tratados de acordo com legislação específica, que contenha medidas proporcionais e necessárias para que o tratamento de dados pessoais atenda ao interesse público.

É possível, com essa previsão legal, que os Poderes públicos compartilhem, entre si, os dados pessoais.

No Capítulo V da referida Lei, são estabelecidos os requisitos e a possibilidade para a transferência internacional de dados, que apenas é permitida aos países ou organismos que tenham um grau de proteção de dados pessoais compatíveis com o que a Lei brasileira prevê. São estabelecidas, também, as formas como o controlador pode garantir o cumprimento das garantias e dos princípios a que o titular dos dados tem direito, conforme o inciso II do art. 33: “[...] a) cláusulas contratuais específicas para determinada transferência; b) cláusulas-padrão contratuais; c) normas corporativas globais; d) selos, certificados e códigos de conduta regularmente emitidos” (BRASIL, [2020b], documento *on-line*). Portanto, pode-se entender que as pessoas jurídicas de direito público poderão requerer que a Autoridade Nacional de Proteção de Dados (ANPD) avalie o nível de proteção de dados pessoais conferido por país ou organismo internacional para possibilitar o correto envio de dados. É o controlador quem deve garantir esse envio dentro da legalidade.

O art. 33 traz, conforme a LGPD, Brasil ([2020b], documento *on-line*), ainda, o seguinte:

[...] II — quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;

IV — quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

V — quando a autoridade nacional autorizar a transferência;

VI — quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

VII — quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;

VIII — quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou

IX — quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.

Mais uma vez, é importante chamar a atenção para o consentimento do titular, de forma livre, informada e inequívoca para uma finalidade determi-

nada. Ou seja, o consentimento não pode conter qualquer tipo de coerção, devendo, o titular, também ser informado sobre a possibilidade de negar essa autorização e as possíveis consequências da negativa. A finalidade sempre deve ser clara e, havendo mais de uma, devem ser explanadas em separado, com as devidas aceitações.

Considerando que a transferência internacional de dados pode ser discutida internacionalmente, para que seja legal, em um contrato, deve respeitar os termos da Lei nº 9.307, de 23 de dezembro de 1996, conhecida como a “Lei da Arbitragem”. Isso garantiria o processo probatório, evitando qualquer possibilidade de cerceamento de defesa. A LGPD tem, como princípio, a promoção de garantias e mecanismos protetivos aos direitos dos titulares; por isso, se um país ou organismo receptor dos dados transferidos não demonstrar o mesmo nivelamento de proteção, serão colocados em risco direitos e liberdades fundamentais legalmente protegidas no Brasil. O *Guia de Boas Práticas da LGPD*, Advocacia-Geral da União (2020), esclarece o art. 34 da LGPD, afirmando que o nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado será avaliado pela ANPD, que levará em consideração:

- as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;
- a natureza dos dados;
- a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos na LGPD;
- a adoção de medidas de segurança previstas em regulamento;
- a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais;
- outras circunstâncias específicas relativas à transferência.

O Brasil ainda não reconheceu qualquer outro país como tendo o desejado nível de proteção. Da mesma forma, também não teve esse reconhecimento por parte de autoridades estrangeiras. Assim, a transferência internacional de dados deve ser avaliada caso a caso, possibilitando a autorização ou a medida compensatória a ser adotada.



Exemplo

O WhatsApp foi comprado pelo Facebook em 2014. No início de 2021, usuários começaram a ser notificados que haveria compartilhamento de dados entre essas duas plataformas. Isso levaria a uma alteração nos termos de uso do aplicativo, de modo que o usuário seria obrigado a concordar para continuar utilizando as funcionalidades. De uma forma geral, as reações foram negativas, e houve uma migração em massa para outros aplicativos de troca de mensagens. Isso fez com que as modificações não fossem implementadas. A Alemanha, por exemplo, declarou que essa integração é ilegal, ferindo a GDPR.

Referências

ADVOCACIA GERAL DA UNIÃO. *Guia de boas práticas: Lei Geral de Proteção de Dados (LGPD)*. Brasília: Advocacia Geral da União, 2020. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaLGPD.pdf>. Acesso em: 29 abr. 2021.

BRASIL. Conselho da Justiça Federal. *Enunciado 531*. A tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento. VI Jornada de Direito Civil. Coordenador-Geral: Ministro Ruy Rosado de Aguiar. Brasília: Conselho da Justiça Federal, [2013]. Disponível em: <https://www.cjf.jus.br/enunciados/enunciado/142>. Acesso em: 28 abr. 2021.

BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil de 1988*. Brasília: Presidência da República, [2020a]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 28 abr. 2021.

BRASIL. *Lei nº 8.078, de 11 de setembro de 1990*. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília: Presidência da República, [2017]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 28 abr. 2021.

BRASIL. *Lei nº 12.414, de 9 de junho de 2011*. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília: Presidência da República, [2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 28 abr. 2021.

BRASIL. *Lei nº 12.527, de 18 de novembro de 2011*. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília: Presidência da República, [2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 28 abr. 2021.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 28 abr. 2021.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, [2020b]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 28 abr. 2021.

BRASIL. Ministério da Economia. *Guia de elaboração de inventário de dados pessoais: Lei Geral de Proteção de Dados Pessoais*. Brasília: Ministério da Economia, 2020c. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaInventario.pdf>. Acesso em: 28 abr. 2021.

BRASIL. Supremo Tribunal Federal. *Recurso Extraordinário RE 1010606/RJ*. Direito Civil. Responsabilidade Civil. Indenização por Dano Material. Direito de Imagem. Recorrido: Globo Comunicação e Participações S/A. Recorrente: Nelson Curi e outro(a/s). Relator: Ministro Dias Toffoli, 14 de novembro de 2016. Disponível em: <http://www.stf.jus.br/portal/processo/verProcessoDetalhe.asp?incidente=5091603>. Acesso em: 29 abr. 2021.

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. *Revista Espaço Jurídico*, v. 12, n. 2, p. 91-108, 2011. Disponível em: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315>. Acesso em: 28 abr. 2021.

DONEDA, D. C. M. et al. Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. *Pensar: Revista de Ciências Jurídicas*, v. 23, n. 4, p. 1-17, 2018. Disponível em: <https://doi.org/10.5020/2317-2150.2018.8257>. Acesso em: 28 abr. 2021.

FRAZÃO, A. Dados, estatísticas e algoritmos. *Jota*, 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/dados-estatisticas-e-algoritmos-28062017>. Acesso em: 28 abr. 2021.

HOFFMANN-RIEM, W. Controle do comportamento por meio de algoritmos: um desafio para o Direito. *Revista Direito Público*, v. 16, p. 123-162, 2019. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3647>. Acesso em: 28 abr. 2021.

LANEY, D. Gerenciamento de dados 3-D: controle de volume, velocidade e variedade de dados META Group Inc. *Gartner*, 2001.

LYON, D. (ed.). *Surveillance as social sorting: privacy, risk, and digital discrimination*. New York: Routledge, 2003.

MOREIRA, P. B. Direito ao esquecimento. *Revista de Direito*, v. 7, n. 2, p. 293-317, 2016. Disponível em: <https://periodicos.ufv.br/revistadir/article/view/1572>. Acesso em: 28 abr. 2021.

NARAYANAN, A. et al. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton: Princeton University Press, 2016.

PINHEIRO, P. P.; HAIKAL, V. A. A nova lei de crimes digitais. *Gazeta do Povo*, 2013. Disponível em: <https://www.gazetadopovo.com.br/vida-publica/justica-direito/artigos/a-nova-lei-de-crimes-digitais-evf935c0vqjw7rh9b4cq75tfy/>. Acesso em: 28 abr. 2021.

PORTO, A. M.; LIMA JÚNIOR, J. M.; SILVA, G. B. Tecnologia Blockchain e Direito Societário: aplicações práticas e desafios para a regulação. *Revista de Informação Legislativa*, v. 56, n. 223, p. 11-30, 2019. Disponível em: https://www12.senado.leg.br/ril/edicoes/56/223/ril_v56_n223_p11.pdf/view. Acesso em: 28 abr. 2021.

SARLET, I. W. *Dignidade (da pessoa) humana e os direitos fundamentais na Constituição Federal de 1988*. 10. ed. Porto Alegre: Livraria do Advogado, 2015.

SILVA, A. R. S. S.; SOUSA, I. P. Blockchain e smart contracts: os impactos das novas tecnologias no direito. *Revista Brasileira de Direito e Gestão Pública*, v. 7, n. 5, p. 53-66, 2019. Disponível em: <https://editoraverde.org/gvaa.com.br/revista/index.php/RDGP/article/view/7341>. Acesso em: 28 abr. 2021.

SUPREMO TRIBUNAL FEDERAL. STF conclui que direito ao esquecimento é incompatível com a Constituição Federal. *Supremo Tribunal Federal*, 2021. Disponível em: <http://stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=460414>. Acesso em: 29 abr. 2021.

Leituras recomendadas

FERNANDES, R. V. C.; COSTA, H. A.; CARVALHO, A. G. P. (coord.). *Tecnologia jurídica e direito digital: I Congresso Internacional de Direito e Tecnologia* — 2017. Belo Horizonte: Fórum, 2018.

MARTINI, S. R.; BERGSTEIN, L. G. Aproximações entre o direito ao esquecimento e a lei geral de proteção de dados pessoais (LGPD). *Revista Científica Disruptiva*, v. 1, n. 1, p. 160-176, 2019. Disponível em: <http://revista.cers.com.br/ojs/index.php/revista/article/view/14>. Acesso em: 28 abr. 2021.

NAKAMOTO, S. Bitcoin: a peer-to-peer electronic cash system. *Bitcoin*, 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 28 abr. 2021.

NUNES, D. H.; LEHFELD, L. S. Cidadania digital: direitos, deveres, lides cibernéticas e responsabilidade civil no ordenamento jurídico brasileiro. *Libertas: Revista de Pesquisa em Direito da UFOP*, v. 4, n. 2, p. 1-12, 2018. Disponível em: <https://periodicos.ufop.br:8082/pp/index.php/libertas/article/view/1300>. Acesso em: 28 abr. 2021.



Fique atento

Os links para sites da web fornecidos neste capítulo foram todos testados, e seu funcionamento foi comprovado no momento da publicação do material. No entanto, a rede é extremamente dinâmica; suas páginas estão constantemente mudando de local e conteúdo. Assim, os editores declaram não ter qualquer responsabilidade sobre qualidade, precisão ou integralidade das informações referidas em tais links.

Direito Digital e contratos virtuais

Objetivos de aprendizagem

Ao final deste texto, você deve apresentar os seguintes aprendizados:

- Analisar os institutos jurídicos de Direito Digital.
- Definir responsabilidade civil e dano moral no contexto do Direito Digital.
- Reconhecer as características e a autenticidade dos contratos e das assinaturas digitais.

Introdução

Neste capítulo, você vai estudar os principais institutos de Direito Digital e os contratos virtuais. Você vai ver também as principais fontes do Direito, visto que o Direito Digital não tem um código como o Código Penal, por exemplo. O ordenamento jurídico brasileiro, assim, tem normas próprias, que abarcam parte da matéria. Quando não é possível a aplicação de uma norma positivada, recorre-se a outra fonte de Direito.

Até 2014, a maior parte dos conflitos que versavam sobre responsabilidade civil e danos morais envolvendo o contexto digital era solucionada com base, exclusivamente, na jurisprudência. Havia insegurança quanto às decisões, pois cada Tribunal podia firmar um entendimento diferente, ainda que a matéria discutida fosse a mesma. Com o Marco Civil Regulatório da Internet, Lei nº. 12.965, de 23 de abril de 2014, foram normatizadas questões sobre danos e responsabilidades, de modo que, em conjunto com a aplicação dos dispositivos legais civis, é possível formar decisões mais consistentes. Essa segurança também serve de embasamento para setores que trabalham com *compliance* e setor consultivo.

Tratando-se de contratos, por regra, eles devem obedecer às instituições normativas pertinentes ao Direito Civil. Por serem estabelecidas entre pessoas — físicas ou jurídicas —, as relações de contrato são consideradas privadas. Por isso, os contratos virtuais observam a legislação correspondente dos contratos, inclusive quando a relação é de consumo. Ainda, devem estar mais atentos para a questão da segurança da transação em todos os sentidos.

1 Institutos jurídicos de Direito Digital

Uma sociedade é composta por vários indivíduos, que convivem em um mesmo espaço com objetivos em comum. As relações estabelecidas entre as pessoas sofrem interferência de uma série de fatores, como tempo, lugar e cultura. O Direito, nesse sentido, surge como um meio para garantir que as condutas dos indivíduos possibilitem uma vida social em harmonia, com regramentos estabelecidos de acordo com as necessidades, visando à justiça social e ao bem-estar coletivo. O Estado, então, cria normas de conduta para garantir a ordem social. Esses regramentos vão compor o ordenamento jurídico. Como o próprio nome diz, trata-se da ordem normativa jurídica que existe em determinado lugar e tem como origem o exercício do poder estatal.

É sempre bom lembrar que o ordenamento jurídico não é estático, nem perpétuo. Ele precisa acompanhar as transformações da sociedade. O Direito tem essa característica dinâmica, pois precisa conduzir as relações entre os indivíduos, e também com o Estado, por meio do ordenamento jurídico. Isso justifica por que alguns regramentos deixam de existir ao longo do tempo, ou são reformados, ou totalmente substituídos.



Exemplo

Até 2005, o Código Penal brasileiro (CP) previa, em seu art. 240, a criminalização do adultério, que foi revogada pela Lei nº. 11.106, de 28 de março de 2005. Tal crime era previsto na legislação brasileira desde a época do colonialismo, até que se entendeu que não havia mais sentido em manter o dispositivo penal na sociedade atual. Diversos fatores provocaram mudanças nos valores da sociedade brasileira em relação à interferência do Estado para resguardar o monopólio conjugal.

Da mesma forma, as transformações ocorridas na sociedade fazem surgir novos regramentos, como os que se referem ao Direito Digital. Esses regramentos essenciais são considerados institutos de Direito, em outras palavras, são as regras destinadas à aplicação em determinado ramo do Direito, para estabelecer condutas, deveres, limitações e punições.

Para melhor entendermos os institutos de Direito Digital, precisamos abordar rapidamente as **fontes do Direito**. Miguel Reale (2003) considera que as fontes do Direito são forças que tornam uma regra de cumprimento obrigatório, ou seja, aquilo que está positivado pode ser exigido. As fontes de Direito são as origens da norma que irá integrar o ordenamento jurídico. Pode-se chamar de **fonte material** do Direito aquela que diz respeito aos aspectos de onde surgiu um regramento, de modo que se relaciona com a autoridade que elaborou a norma, o tipo de cultura do lugar, aspectos axiológicos, religiosos e temporais. Quando se fala em **fonte formal** do Direito, trata-se do meio de manifestação das fontes materiais, que farão com que determinado componente do ordenamento jurídico seja executado.

As fontes formais podem ser de dois tipos. Veja a seguir.

■ **Diretas:**

- leis e tratados internacionais, observada a hierarquia normativa;
- precedentes, que são decisões com efeito vinculante, desde a edição da Emenda Constitucional nº. 45, de 30 de dezembro de 2004, que criou a figura da súmula vinculante, tornando obrigatória a sua observância aos julgadores.

■ **Indiretas:** são aquelas que suprem a falta da lei. No Brasil são admitidas as seguintes:

- analogia, que é aplicar a um caso concreto algo com semelhanças legais;
- costumes, que são práticas reiteradas de determinada conduta de maneira uniforme e constante, reconhecida pelos membros da comunidade;
- princípios gerais do Direito, que são preceitos fundamentais que, mesmo não escritos, são considerados essenciais para o Direito, como a noção de igualdade, justiça etc.;

- jurisprudência, que são as decisões reiteradas pelos Tribunais em determinada matéria;
- doutrina, que são os embasamentos teóricos;
- negócio jurídico, quando não contrário à lei, obedecendo às formalidades, quando existe, estabelecido entre as partes, como um contrato, por exemplo.

No Brasil, os institutos de Direito Digital utilizam como fonte, de maneira mais vasta, as fontes formais indiretas, porque há pouco regramento estabelecido por leis específicas. Por isso, a analogia, os costumes, os princípios, a jurisprudência e o negócio jurídico se inserem no ordenamento jurídico deste ramo.

Imagine que uma empresa multinacional contrata um profissional para atuar na área de *compliance*. Suas atribuições serão adequar as políticas de uso do ambiente virtual pelos colaboradores às diretrizes de segurança com relação às transações comerciais realizadas. Além do conhecimento sobre legislação internacional nessa área, esse profissional deverá conhecer as leis locais, mas nem todos os dilemas estarão abarcados nela. Veja, se por um lado se deve fiscalizar o conteúdo das transações internacionais realizadas pelos colaboradores por causa da responsabilidade do empregador decorrente dessa relação, por outro, não é possível o monitoramento ostensivo dos funcionários sob pena de infringir a legislação trabalhista, além de ofender direitos fundamentais, como a privacidade e a liberdade. Então, o profissional responsável pelo *compliance* deverá procurar o equilíbrio, consultando os limites entre direitos e deveres que estão dispostos na jurisprudência, na doutrina e nas demais fontes formais indiretas, inclusive se valendo da analogia a leis que possam conferir segurança ao funcionamento da empresa.

O Direito Digital se utiliza de inúmeras conexões com áreas do Direito, como o Direito Civil, o Direito Penal, o Direito Trabalhista, o Direito Consumerista, o Direito Internacional e o Direito Ambiental.



Exemplo

Os aplicativos de transporte surgiram como uma alternativa ao uso do táxi. O primeiro serviço desse tipo chegou ao Brasil em 2014, com grande adesão da sociedade, o que gerou um tipo de concorrência até então inexistente para os taxistas. A Lei nº 12.587, de 3 de janeiro de 2012, não tratava sobre esse assunto, mas a sociedade já estava usufruindo dos benefícios e vantagens que essa transformação digital proporcionava.

Em 2018 surgiu a Lei nº. 13.640, de 26 de março de 2018, que conferiu aos Municípios e ao Distrito Federal a competência exclusiva para regulamentar e fiscalizar o serviço de transporte remunerado privado individual de passageiros, obedecendo a alguns critérios. Este é um caso em que o ordenamento jurídico precisou incorporar uma norma para definir padrões de conduta dentro da sociedade.

Fonte: Vasconcelos e Assis (2018).

Principais instituições de Direito Digital

O inciso segundo do art. 5º da Constituição Federal diz que “[...] ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei” (BRASIL, 1988, documento *on-line*). Este é o dispositivo conhecido como **princípio da legalidade**, cuja aplicação fundamental consiste em dizer que apenas a lei pode justificar a imposição a uma pessoa de fazer ou deixar de fazer algo. As condutas são reguladas e limitadas em decorrência das normas instituídas, por isso, as instituições de Direito dizem respeito à legislação que se aplica, ou que se instituiu.

Com o Direito Digital não é diferente. As instituições legais consistem em regramentos específicos para a conduta nesse campo. O Direito Digital tem uma legislação distribuída em diversas áreas e legislação própria. A seguir estão os principais regramentos que compõem as instituições de Direito Digital.

- **Decreto nº. 7.962/2013:** o Decreto nº. 7.962, de 15 de março de 2013, regulamentou o Código de Defesa do Consumidor para dispor sobre a contratação no comércio eletrônico. Estabeleceu regras para o direito de arrependimento, cumprimento da oferta e informações fornecidas ao consumidor.

- **Lei nº. 12.737/2012:** a Lei nº. 12.737, de 30 de novembro de 2012, modificou o CP para inserir os arts. 154-A e 154-B, criminalizando a invasão de dispositivos eletrônicos. Também alterou os arts. 266 e 298, sobre perturbação ou interrupções de prestação de serviço digital e clonagem de dados bancários e cartões de crédito por meio virtual, respectivamente. Esta lei é conhecida pelo apelido de Lei Carolina Dieckmann, pois foi aprovada depois de um episódio envolvendo violação da privacidade digital da atriz. O projeto, todavia, é bem anterior ao fato, de modo que, originalmente, buscava proteger dados vinculados aos poderes do Estado.
- **Lei nº. 12.965/2014:** a Lei nº. 12.965, de 23 de abril de 2014, é chamada de Marco Civil Regulatório da Internet. Até o seu surgimento, não existia no ordenamento jurídico brasileiro uma legislação que se ocupasse em diferenciar as responsabilidades e as práticas na internet, principalmente quanto aos provedores e prestadores de serviço de internet. Em seu art. 1º, a lei diz que se presta a estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil e determinar as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria. Além disso, a lei se baseia na liberdade de expressão como basilar e traz como inovação a determinação da neutralidade de rede e promoção da internet a todos.
- **Lei nº. 13.709/2018:** sob a influência da publicação do Regulamento Geral de Proteção de Dados da União Europeia (GDPR), o Brasil aprovou a sua Lei Geral de Proteção de Dados (LGPD), a Lei nº. 13.709, de 14 de agosto de 2018. Esta lei regulamenta o uso, a proteção e a transferência de dados pessoais, e determina quem são os agentes envolvidos e suas atribuições de responsabilidades por incidentes, sejam eles públicos, sejam privados. Há sanções previstas para quem descumprir os seus preceitos, uma vez que pode determinar multas baseadas no grupo econômico em que a empresa infratora está inserida. Outra novidade desta lei é a criação da Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal.



Fique atento

Com o surgimento das leis de proteção de dados, tanto a europeia quanto a brasileira, diversas empresas estão alterando seus termos de uso e política de privacidade para atender aos requisitos legais. Por isso, ao fornecer seus dados pessoais, é importante que você leia esses documentos e conheça a finalidade, o tratamento e a destinação que ali estão expostos. É uma obrigação da empresa que coleta dados pessoais informar ao usuário todas as possibilidades de uso dos dados — afinal, é sempre quem fornece os dados que informa que está ciente e aceita os termos.

2 Responsabilidade civil e dano moral no contexto digital

Dentro de um enfoque digital, a responsabilidade civil e o dano moral seguem as premissas estipuladas no Código Civil (CC), Lei nº. 10.406, de 10 de janeiro de 2002. Para compreendermos o conceito, precisamos conhecer o que dizem seus artigos combinados 186, 187 e 927 do CC. O art. 186 refere que, quem causar dano a outra pessoa, mesmo que apenas moral, comete um ato ilícito por sua conduta, seja ela uma ação ou uma ação voluntária, seja negligência ou imperícia. O art. complementa, incluindo no ato ilícito aqueles exercidos com excesso pelo titular de um direito.

No art. 927 o CC estipula que o responsável pelos atos ilícitos que causaram danos a outra pessoa é obrigado, ou seja, é titular da obrigação de reparar tais danos. O parágrafo único desse artigo fala sobre a obrigação de reparar o dano, independentemente de comprovação de culpa quando houver previsão legal ou quando a atividade habitualmente desenvolvida por quem causou o dano implicar, por sua natureza, risco para os direitos de outrem.

A legislação civil vai direcionar os seus objetivos à reparação patrimonial, ou seja, quem tiver diminuído o seu patrimônio por uma ofensa causada por outra pessoa terá direito a receber uma indenização para repor aquilo que perdeu. Isso pode ser facilmente visualizado pensando-se, por exemplo, em um acidente de automóvel, no qual o causador deve indenizar a parte que sofreu prejuízo arcando com os custos do reparo do veículo. Este é um caráter patrimonial objetivo, porque se pode quantificar. Existe outro caráter de dano, que é subjetivo, este se chama dano moral. O **dano moral** decorre de uma ofensa cujo resultado pode não ser apenas patrimonial, mas íntimo, como uma ofensa à honra e boa imagem, por exemplo.

Nos artigos, podemos verificar que o legislador considerou obrigado a indenizar o outro aquele que comete ato ilícito. Os arts. 186 e 187 definem o que se considera ato ilícito. Nos termos da lei civil, **atos ilícitos** são **condutas omissivas** (deixar de fazer) ou **comissivas** (fazer) que causam prejuízo material ou moral, sendo que o moral será de avaliação subjetiva do ofendido. O art. 186 traz uma informação importante que será utilizada para avaliar a culpabilidade do agente, quando menciona que o ato é ilícito pela ausência do cuidado que deveria se ter (**negligência e imprudência**).



Saiba mais

Veja a seguir a diferença entre cada termo e seu significado.

- **Imperícia:** é inaptidão, ignorância, falta de qualificação técnica, teórica ou prática, ou ausência de conhecimentos elementares e básicos da profissão.
- **Negligência:** é deixar de tomar uma atitude ou não apresentar conduta que era esperada para a situação.
- **Imprudência:** pressupõe uma ação precipitada e sem cautela.

Fonte: São Paulo (2017, documento *on-line*).

O dever de indenizar será mensurado monetariamente, levando em consideração a quantificação do dano patrimonial. Em casos de danos morais, há outros fatores a serem observados, como o tamanho da ofensa e o resultado que isso causou na vida do ofendido. Por ser uma questão subjetiva, algo proferido em redes sociais, por exemplo, pode ter diferentes impactos, que dependem da pessoa. Há pessoas que sofrem de patologias, como a depressão, cujo descontentamento ocasionado por alguma ofensa na internet pode gerar como consequências de um abalo maior. Deve-se considerar também o cargo que a pessoa ocupa e a ofensa à honra que pode prejudicar o desempenho das suas funções. Por outro lado, há pessoas cuja vida pública permite maior flexibilização quanto à questão da privacidade.

Quando se quantifica o dano moral, a figura do ofensor é outra variável a ser considerada. É possível atribuir caráter punitivo, de modo que a indenização seja majorada. Por exemplo, em caso de indenização por danos morais ocorridos em rede social de uma grande empresa que ironiza seu consumidor que está com o recebimento da mercadoria atrasada. Ainda que se receba a

mercadoria e não haja dano patrimonial, o dano moral pode ser pedido pela ofensa, para que a empresa seja punida pela conduta.

Considerando uma análise processual sobre o assunto, é possível ajuizar ação requerendo danos morais independentemente do pedido de danos patrimoniais, e vice-versa. Os dois tipos de dano, desde o Código de Processo Civil (CPC), que entrou em vigor no ano de 2016, devem ser quantificados cada qual no pedido. Antes, era possível requerer dano patrimonial por quantia certa e atribuir o arbitramento do dano moral ao Juiz.

O parágrafo único do art. 927 do CC fala em **culpa**. A culpabilidade é um elemento analisado para fins de definição do tipo de responsabilidade. Para que surja o dever de indenizar é necessária a comprovação da existência do dano (seja moral ou material), a ação ou omissão do agente causador do dano e o nexo causal, que é a capacidade da conduta do agente causar ou não a ofensa. O ato ilícito deve ser proporcional ao dano causado para que seja passível de indenizar. Neste ponto se analisa a questão da culpabilidade, ou seja, a prova do grau de responsabilidade do ofensor pelo dano. O que o parágrafo único traz é que existe um tipo de responsabilidade, chamada objetiva, na qual surge o dever de indenizar, sendo dispensada a análise da culpabilidade.

A responsabilidade civil tem, então, dois tipos que podem dar origem ao dever de indenizar. Veja a seguir.

- **Responsabilidade civil subjetiva:** na qual se analisa conduta do agente, culpabilidade, nexo causal e dano.
- **Responsabilidade civil objetiva:** na qual se analisa conduta do agente, nexo causal e dano.

Como refere o artigo, a responsabilidade objetiva será oriunda de dispositivo legal, ou seja, a lei irá determinar. É o que ocorre com as relações de consumo: por determinação do Código de Defesa do Consumidor, as responsabilidades por fatos do produto ou do serviço são do fornecedor, cabendo a inversão do ônus probatório.

Em matéria de responsabilidade civil na internet, para fins probatórios, são admitidos os meios digitais. Havendo a prática de ato ilícito no meio digital, é possível constituir prova válida por meio de mensagem, correio eletrônico, vídeo, foto e até mesmo captura de tela, ainda que o ofensor apague posteriormente aquilo que publicou. Por meio de um documento chamado **ata notarial**, elaborado em Tabelionato, será redigido com fé pública uma descrição daquilo que se tem armazenado no meio digital.

A internet não pode ser considerada uma terra sem leis, de modo que os danos morais por ofensas veiculadas nos meios digitais são passíveis de indenização. As redes sociais, principalmente, são veículos de comunicação e informação. Antes do Marco Civil Regulatório da Internet, era discutido se havia responsabilização dos provedores e das redes por conteúdos publicados. Se você pesquisar jurisprudências daquela época encontrará decisões em vários sentidos.

O Marco Civil da Internet explicitou sobre provedores aquilo que a Portaria do Ministério das Comunicações nº. 148, de 31 de maio de 1995, estabelecia: a existência de dois tipos de serviço, o de conexão à internet e o de informações. Neste sentido, definiu que o **serviço de conexão à internet** (ou provedor de acesso/provedor de conexão) é a entidade que proporciona a conexão dos computadores que usam seus serviços à internet. Estes devem possibilitar e garantir a liberdade de expressão sem censura prévia. Desse modo, o provedor de internet não terá responsabilidade civil por danos decorrentes de conteúdo gerado por terceiros conforme o art. 18 do Marco Civil.

Já quanto aos **provedores de conteúdo**, ou de aplicação, o art. 19 do Marco Civil declara que, salvo disposição legal em contrário, estes somente serão responsabilizados por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomarem as providências para, no âmbito do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente. A exceção é quando há casos de divulgação de material contendo nudez ou cenas de sexo, neste caso, a ordem judicial é dispensável. A maior parte das plataformas disponibiliza um mecanismo para que o usuário denuncie este tipo de conduta. Quanto a este tipo de responsabilidade subsidiária, é consenso na jurisprudência que não é objetiva, sendo necessária a análise da culpabilidade.



Saiba mais

O Superior Tribunal de Justiça (STJ) disponibiliza, desde 2017, no [link](#) Pesquisa Pronta, jurisprudência por assuntos relacionados com a responsabilidade civil de provedores de internet. Pesquise “pesquisa pronta stj” em seu mecanismo de busca na internet, que você encontrará facilmente o [link](#) para a página de pesquisa de jurisprudência do STJ.

3 Contratos virtuais

Um contrato pode ser definido como um acordo de vontades, firmado por duas ou mais pessoas, com a finalidade de criar, modificar ou extinguir direitos. Quando se realiza uma compra, constitui-se um contrato de compra e venda e nem sempre é necessária a formalidade escrita. Por exemplo, quando você vai à padaria, apenas pede a quantidade de pães que precisa, efetua o pagamento e o negócio foi feito. Quando há valores maiores envolvidos, como a aquisição de um imóvel, de um veículo ou a contratação de algum serviço, é comum utilizar a forma escrita, para que haja mais segurança. O contrato estabelece os deveres e obrigações das partes por meio das cláusulas e condições, seja ele físico, seja virtual.

Os **contratos virtuais**, embora o CC não preveja explicitamente, devem seguir praticamente os mesmos requisitos dos contratos tradicionais. Algumas formas de contrato virtual são mais familiares, como realizar compras pela internet. Outros tipos contratuais não são tão explícitos, como escolher um plano de telefonia, que é um contrato de prestação de serviço, ou baixar um programa de computador, que é um contrato de licença de uso.



Fique atento

As atuais relações comerciais da era digital trazem uma série de contratos para a vida das pessoas. Pedir comida usando um aplicativo é como ir ao restaurante. Pedir um motorista de aplicativo é como um contrato de transporte. As relações contratuais são similares.

Na área de consumo, a oferta veiculada pela internet vincula o negócio da mesma maneira que as propagandas de promoções feitas nos jornais. As dívidas de contratos virtuais são reconhecidas como existentes, podendo ser cobradas judicialmente.

Os contratos virtuais se regem pelos mesmos princípios básicos dos demais contratos, devendo observar a boa-fê, tanto na celebração do ato quanto em sua execução, como assegura Pinheiro (2013). A vontade dos contratantes deve ser expressa livremente, sem que sejam coagidos ou induzidos a erro. Outro fator importante é a capacidade de negociar as cláusulas e condições contratuais. Quando isso não ocorre, o contrato é chamado de **adesão**. É uma prática comum em contratações de serviços nos quais uma das partes apenas concorda e assina aderindo aos seus termos. O direito reconhece este contrato como passível de revisão ou de interpretação mais favorável à parte aderente, é o que acontece de maneira comum em relações de consumo.

Quanto aos requisitos contratuais, devem ser observados aqueles dispostos no art. 104 do CC, pois são negócios jurídicos. Veja a seguir.

- **Agente capaz:** aqueles que contratam devem ter capacidade jurídica e civil para tal. Se for pessoa física, ser maior, capaz, ou ter procuração, representação e etc. Se for pessoa jurídica, o representante legal, o preposto autorizado, o sócio, o administrador e demais figuras.
- **Objeto lícito, possível, determinado ou determinável:** diz respeito ao objeto da contratação, não se pode elaborar contratos com objetos ilícitos ou impossíveis. No que diz respeito à determinação, se não for possível estabelecê-la ao tempo da assinatura, deve ser determinável ao tempo do cumprimento ou da execução do mesmo.
- **Forma prescrita ou não defesa em lei:** alguns contratos têm formalidades estabelecidas em lei; quando não houver, a regra é que a forma é livre ou não proibida.

Um contrato deverá conter, de maneira clara, quem são as partes, qual seu objeto, a que título é feito, o preço e as condições de pagamento (quando oneroso), prazos de entrega e demais informações que garantam a sua completa perfectibilização. A declaração de vontade e de concordância se dá por meio da assinatura; nos contratos virtuais, muitas vezes, é dado um aceite por meio da concordância dos termos.

Alguns contratos requerem assinatura digital para comprovar a veracidade e conferir validade ao negócio. Em 2001, por meio da Medida Provisória nº. 2002-2, de 24 de agosto de 2001, foi criado um sistema de chaves conhecido como ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras. Por meio desses certificados digitais,

é possível reconhecer assinatura eletrônica de pessoas físicas e jurídicas pelo seu dispositivo móvel ou computador, utilizando *token* ou sistemas de *log-in* e senha. Tais aplicações são amplamente utilizadas para emissão de notas fiscais eletrônicas, questões tributárias e contratações internacionais.

Os contratos eletrônicos podem ser classificados em três categorias, listadas a seguir.

1. **Intersistêmicos:** são aqueles utilizados entre as empresas, por meio de uma rede fechada de comunicação, utilizando sistemas e aplicativos programados para esta finalidade. A comunicação não acontece entre empresas e consumidor, apenas entre os sistemas empresariais.
2. **Interpessoais:** é a contratação que ocorre entre as partes que, por meio digital, em ambiente virtual, instrumentalizam a contratação.
3. **Iterativos:** são os mais comuns, firmados entre um sistema operacional e uma pessoa, por meio de *site* ou loja virtual. Neste caso, o Código de Defesa do Consumidor pode ser aplicado.



Exemplo

Quando se veicula uma propaganda de algo fora dos meios digitais, é necessário expor todas as informações referentes ao anúncio. Muitas vezes, a imagem do produto anunciado não é a do produto objeto da promoção. Por exemplo, o anúncio de um carro pode exibir a imagem de um modelo com opcionais e a promoção se referir ao modelo de fábrica. Esse recurso é utilizado para chamar a atenção do consumidor. Para que não induza ao erro, é preciso avisar que a imagem é meramente ilustrativa e que inclui opcionais a que a promoção não se aplica. A oferta veiculada em meios digitais deve obedecer a esses princípios também para que não seja considerada propaganda enganosa.

Analisando o conteúdo abordado, podemos percorrer uma sequência lógica de entendimento sobre os institutos de Direito Digital e contratos virtuais. O Direito Digital é dinâmico e as novidades são apresentadas para a sociedade de modo que passam a fazer parte da vida das pessoas antes mesmo dos regramentos jurídicos sobre elas. Por isso há possibilidades de aplicação e interpretação dentro do Direito Digital que permitem uma vida equilibrada com esses movimentos tecnológicos.

Ao conhecermos as instituições de Direito Digital, podemos aplicá-las de forma adequada à preservação da organização social, à manutenção e à limitação dos deveres e direitos. As responsabilidades civis no contexto digital e os danos morais que têm relação com danos causados em ambiente virtual podem ser reconhecidos, e as medidas cabíveis para reparação ou, antes disso, para evitar que aconteçam, são fundamentais para o exercício da cidadania. Da mesma forma, os contratos virtuais, com suas peculiaridades e requisitos, são uma realidade na sociedade moderna. Dominar os recursos e cuidados que esta modalidade requer é uma maneira de assegurar a boa prestação da finalidade contratual.



Referências

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil*. Brasília: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 22 ago. 2020.

BRASIL. *Lei nº 10.406, de 10 de janeiro de 2002*. Instituiu o Código Civil. Brasília: Presidência, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm. Acesso em: 22 ago. 2020.

BRASIL. *Lei nº 12.737, de 30 de novembro de 2012*. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Brasília: Presidência, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 22 ago. 2020.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Presidência, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 22 ago. 2020.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília: Presidência, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 22 ago. 2020.

PINHEIRO, P. P. *Direito digital*. 5. ed. São Paulo: Saraiva, 2013.

REALE, M. *A teoria tridimensional do Direito*. Lisboa: Imprensa Nacional: Casa da Moeda, 2003.

SÃO PAULO. Tribunal de Justiça. #Glossário #Imperícia #Negligência #Imprudência. São Paulo, 13 jun. 2017. Twitter: @TJSPoficial. Disponível em: <https://twitter.com/TJSPoficial/status/874719328729432065>. Acesso em: 22 ago. 2020.

VASCONCELOS, G. C.; ASSIS, N. G. O serviço público de transporte de passageiros e os aplicativos de motoristas particulares. *In: CONGRESSO INTERDISCIPLINAR DE PESQUISA, ENSINO E EXTENSÃO*, 2., 2018, Belo Horizonte. *Anais* [...]. Belo Horizonte: Centro Universitário Metodista Izabela Hendrix, 2018. Disponível em: <http://izabelahendrix.edu.br/pesquisa/anais/PginasdeAnais201821.p.512p.528.pdf>. Acesso em: 26 ago. 2020.

Leituras recomendadas

GONÇALVES, V. H. P. *Marco civil da internet comentado*. São Paulo: Atlas, 2017.

RAMINELLI, F. P.; RODEGHERI, L. B. A proteção de dados pessoais na internet no Brasil: Análise de decisões proferidas pelo Supremo tribunal Federal. *Cadernos do Programa de Pós-Graduação em Direito/UFRGS*, v. 11, n. 2, p. 89–119, 2016. Disponível em: <http://seer.ufrgs.br/ppgdir/article/view/61960/39936>. Acesso em: 22 ago. 2020.



Fique atento

Os *links* para *sites* da *web* fornecidos neste capítulo foram todos testados, e seu funcionamento foi comprovado no momento da publicação do material. No entanto, a rede é extremamente dinâmica; suas páginas estão constantemente mudando de local e conteúdo. Assim, os editores declaram não ter qualquer responsabilidade sobre qualidade, precisão ou integridade das informações referidas em tais *links*.

Criptografia e assinaturas digitais

Objetivos de aprendizagem

Ao final deste texto, você deve apresentar os seguintes aprendizados:

- Explicar conceitos de segurança e privacidade.
- Identificar exemplos de criptografia e suas aplicações.
- Descrever os tipos e usos de assinaturas digitais.

Introdução

Certamente você já deve ter utilizado sua conta de rede social ou de *e-mail* para se cadastrar em algum serviço automaticamente. Ao utilizar esses mecanismos de autenticação (conhecidos como OAuth2), algumas questões podem ser consideradas, como quais acessos foram concedidos ao sistema, que tipo de privacidade é utilizada e quais informações de fato ele necessita ter.

Além das questões de usuários e privacidade, como tópicos de segurança, é comum que sistemas troquem informações entre si, consumam serviços uns dos outros e disponibilizem acessos para diversos fins. Por exemplo, considere que um ambiente de *cloud computing* (computação em nuvem) disponibiliza diretamente acesso a um banco de dados de clientes, se o acesso for aberto, autenticado por usuário e senha, existe a possibilidade de um ataque do tipo “força bruta” (quando o atacante testa diversas combinações de usuário e senha até que acerte).

Neste capítulo, você compreenderá questões gerais de segurança da informação, que incluem privacidade de usuário.

1 Segurança e criptografia

Não faz sentido discorrer sobre criptografia, assinaturas digitais e meios de comunicação, sem que se compreenda o que a segurança significa no contexto em que estamos inseridos. Segurança da informação em meios computacionais está ligada a três pilares fundamentais que, quando trabalham em conjunto, tornam possível dizer que determinado sistema está seguro.

O primeiro dos três pilares é a **confidencialidade**, cujo princípio é que qualquer dado ou informação acessados atendam apenas quem os pode acessar. Obviamente, para que haja, de fato, um controle rígido de acesso, é preciso um controle de usuários e permissões. O segundo é a **disponibilidade**, na qual o dado ou a informação deve estar disponível quando for requisitado. Já o terceiro pilar é a **integridade**, por exemplo, se considerarmos um arquivo, que não pode ser alterado ou modificado indevidamente.

Portanto, você pode pensar cada um dos três pilares, considerando os seguintes contextos: a confidencialidade é verificada quando, por exemplo, somente você consegue acessar os arquivos que armazenou em nuvem; a disponibilidade, quando seus arquivos estão, de fato, a sua disposição no momento necessário; e a integridade, ou melhor, a falta dela, é notada em uma situação em que, hipoteticamente, você faz o *download* de algum arquivo na internet e ele está corrompido.

Existem autores que ainda adicionam mais dois pilares, tornando o entendimento de segurança mais complexo e robusto. Um deles é a autenticidade, nem sempre mencionada na internet ou em outras literaturas, mas que é relevante no contexto de sistemas distribuídos abordado neste capítulo. A autenticidade é entendida como a garantia de que a fonte geradora da informação é, de fato, quem alega ser. Você já deve ter recebido algum e-mail de um conhecido que alega não o ter enviado. Isso é muito comum entre alguns vírus de computador que utilizam a agenda da vítima para enviar e-mails diversos. Esse é um ótimo exemplo de autenticidade: o remetente é quem você conhece, mas ele desconhece a mensagem ou o envio dela. Por fim, o último dos pilares “extras” é a legalidade, presente no contexto em que a informação ou dado respeita leis vigentes no país no qual está hospedada.



Saiba mais

No Brasil existem algumas leis, já implantadas ou ainda em tramitação, que regem questões de legalidade. Conheça essas leis e como elas podem influenciar em seu sistema distribuído ou *software* pesquisando na internet sobre o Marco Civil da Internet no Brasil (Lei nº. 12.965/2014) e sobre a Lei Geral de Proteção de Dados.

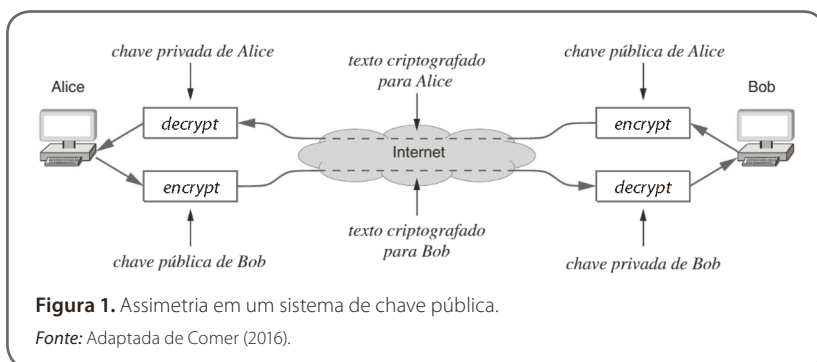
Os princípios básicos de confidencialidade, integridade, disponibilidade, autenticidade e legalidade (CIDAL) é um direcionador teórico sobre o necessário para um sistema (seja ele distribuído ou não) ser considerado seguro. Com essa definição teórica dos postos-chave para que haja segurança, podemos discutir agora o que é criptografia. Quando criança, ou mesmo depois de adulto, você já deve ter feito piadas internas ou que só fazem sentido para algumas pessoas de seu círculo social. É possível interpretar a criptografia com essa analogia: em uma roda de amigos e conhecidos, apenas essas pessoas conseguem compreender determinada mensagem por já saberem do que se trata.

A criptografia tem valor histórico no desenvolvimento da humanidade e foi amplamente utilizada em guerras. Caso nunca tenha ouvido falar, o filme “O jogo de imitação” conta a história de Alan Turing, pai da computação, e da primeira máquina (que anos depois seria caracterizada como o primeiro computador) criada para desvendar códigos criptográficos da Enigma (mecanismo alemão que criava cifras de criptografia durante a Segunda Guerra Mundial), utilizada até hoje como referência. Para melhor compreender esse processo, Comer (2016, p. 451) apresenta alguns itens de terminologia de criptografia:

[...] Texto aberto – uma mensagem original antes de sido criptografada. Texto cifrado – uma mensagem após ter sido criptografada. Chave de criptografia – um conjunto curto de bits usado para criptografar uma mensagem. Chave de descryptografia – um conjunto curto de bits usado para descryptografar uma mensagem. [...]

A criptografia é um processo relativamente simples e que envolve uma chave e uma mensagem. Apesar do processo ser simples, o algoritmo utilizado para realizá-lo pode não ser tão simples assim (lembrando que algoritmo é uma sequência de comandos praticados por um programa ou usuário). Como Comer (2016) apresenta, entre as diversas técnicas de criptografia, existem basicamente duas categorias que podem ser utilizadas.

- Chave privada — cada nó ou participante do grupo tem uma cópia da chave criptográfica que é utilizada tanto para criptografia como para descryptografia.
- Chave pública — existe uma troca de chaves entre os serviços. Como demonstrado na Figura 1, a chave pública de Alice é enviada para Bob, e a chave pública de Bob, para Alice. Isso faz Bob conseguir criptografar todo conteúdo para Alice e apenas ela descryptografar, e vice-versa.



Portanto, a criptografia, apesar de ser um processo simples na teoria, pode ser muito complexa na prática, devido aos algoritmos (normalmente matemáticos) envolvidos. Considerando os pilares já discutidos, é possível perceber que a ideia de confidencialidade é respeitada com o uso de uma criptografia robusta o suficiente para que nenhum atacante ou intermediário consiga descryptografá-las, e nem complexa o bastante para que o usuário deixe de usá-la.



Saiba mais

As famosas moedas criptográficas, ou Bitcoin, só são possíveis por meio de uma criptografia baseada na tecnologia chamada de Blockchain. Essa tecnologia tem sido utilizada em diversas pesquisas que permitam a verificação de dados, como autenticidade de documentos. Entenda um pouco mais sobre essa tecnologia revolucionária assistindo ao vídeo Criptomoedas, Blockchain e Altcoins, do canal do Youtube Nerdologia, e/ou lendo o artigo “Blockchain: entenda o que é e quais são as principais aplicações”, da Exame.

Com base nessas informações sobre segurança e criptografia, pode-se pensar sobre as reais ameaças a um sistema distribuído. Como definido por Tanenbaum e Van Steen (2007), um sistema distribuído tem basicamente quatro tipos de ameaças a considerar:

- **interceptação** — quando a mensagem ou o dado consegue ser adquirido por um terceiro, que não deveria ter acesso a essa informação (ferindo princípios de confidencialidade, legalidade, autenticidade e integridade, dependendo da intenção desse terceiro elemento);
- **interrupção** — quando um serviço, dado ou informação, por algum motivo de ataque, torna-se indisponível, ou seja, inacessível. Nesse contexto, mesmo que haja tolerância a falhas ou replicação de arquivos, eles falharam em sua função. Qualquer dado que, por algum motivo, foi corrompido ou perdido pode ser associado ao problema de interrupção;
- **modificação** — ocorre quando o dado, a informação ou o processo é modificado sem autorização. Uma interceptação de dados pode estar aliada às questões de modificação, pois, se o atacante tem acesso a esses dados, pode ser que também os possa alterar;
- **invenção** — dados ou informações gerados em um contexto em que normalmente não acontecem (exemplo dos *e-mails* falsos).



Fique atento

Além do sistema distribuído ser capaz compreender e entregar todas as características definidas pelo CIDAL, Tanenbaum e Van Steen (2007) destacam que ferramentas de auditoria são importantes. Sistemas que passam por auditorias constantes têm como padrão testar todas as características do CIDAL. Ferramentas sérias de auditoria podem ajudar, inclusive, a precaver diversos tipos de ataques que, dependendo do sistema, são muito comuns.

Segurança da informação é, de fato, um dos principais pilares que podem (e devem) ser utilizados por sistemas distribuídos. É importante lembrar que para um sistema ser considerado seguro, precisa ter a segurança como parte de sua arquitetura e funcionamento. Nesse contexto, deve-se considerar a questão da legalidade no Brasil. Com regras rígidas, determinadas pela Lei Geral de Proteção de Dados, como desenvolvedor ou administrador de um sistema, você está submetido às sanções dessa lei sobre os dados que estão sob sua tutela. Basicamente, se algo acontecer com os dados de clientes que utilizam o seu sistema (seja ele distribuído ou não), você pode ser responsabilizado.

2 Criptografar ou não

Uma vez que a importância da criptografia no sistema distribuído foi definida, surge a questão sobre quais técnicas são úteis e se tudo precisa ser, de fato, criptografado. Comer (2016, p. 453) afirma que, “Se a confidencialidade não for necessária, a mensagem não precisa ser criptografada. Em vez disso, uma forma mais eficiente de assinatura digital pode ser utilizada; por meio dela, somente um *hash* da mensagem é criptografado [...]”. Portanto, não adianta criptografar tudo, é necessário ter coerência, pois todos os nós, pessoas ou dispositivos computacionais que participam do mesmo grupo de troca de mensagens podem não conseguir decifrar a mensagem por falta de configuração, ou falta de necessidade de criptografia.



Fique atento

Quando os algoritmos são referidos em computação, trata-se de uma sequência de comandos processados em uma determinada ordem e que pode ter uma complexidade computacional muito grande. Considerando a complexidade de dados, qualquer algoritmo tem um custo de tempo para ser processado. A complexidade de algoritmo é um modelo matemático que se aproxima da realidade de um processador para calcular o custo da sua utilização na unidade computacional em questão. Pode, também, ser tratada como questões de processamento (quanto um determinado algoritmo consome do processador), memória (quanto de memória principal é utilizada para sua execução) e armazenamento (quanto ele ocupa de disco físico), não devendo ser ignorada em criptografia. Alguns algoritmos podem ter um custo muito maior que sua unidade de processamento é capaz de atender, o que torna seu uso inviável.

Técnicas de criptografia

Antes de analisarmos alguns cenários em que a criptografia é necessária e como pode ser aplicada, observe o Quadro 1 para compreender diversas técnicas de segurança.

Quadro 1. Resumo das principais técnicas e seus objetivos

Técnica	Objetivo
Hashing	Integridade dos dados
Criptografia	Privacidade
Assinatura digital	Autenticação de mensagens
Certificados digitais	Autenticação do transmissor
Túnel	Comunicação criptografada

Fonte: Adaptado de Comer (2016).

A técnica de *hashing* é importante para definir se os dados estão, de fato, íntegros. Para garantir questões de privacidade e autenticidade dos dados são necessários a criptografia, a assinatura digital e os certificados digitais. Vamos abordar alguns sistemas para que você compreenda melhor como a criptografia é utilizada.

O *data encryption standart* (DES), ou padrão de criptografia de dados, é utilizado para operar em sistemas simétricos (TANENBAUM; VAN STEEN, 2007). O DES opera com um padrão de transmissão em rodadas e com criptografia em cada uma delas, ou seja, para cada rodada, ele possui uma chave criptográfica diferente, mas todas sempre derivando de uma chave mestra de 56 bits (COULOURIS *et al.*, 2013). A Figura 2 demonstra esse processo de forma completa, sendo possível visualizar cada uma das 16 rodadas, incluindo a inicial e a final, que são diretamente inversas. Esse tipo de criptografia foi utilizado durante anos e ainda pode ser encontrado em diversos sistemas.

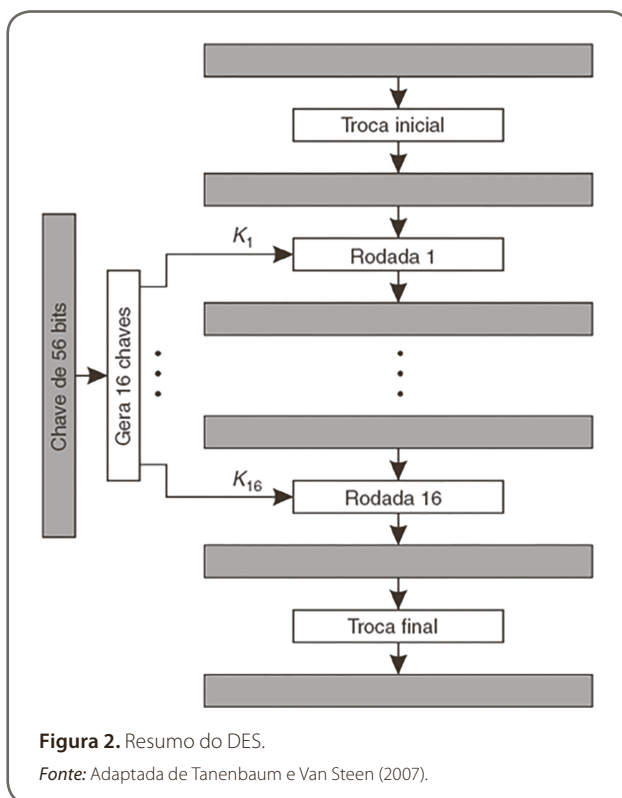


Figura 2. Resumo do DES.

Fonte: Adaptada de Tanenbaum e Van Steen (2007).

Outro padrão de criptografia bastante conhecido é o *Rivest-Shamir-Adleman* (RSA) (GOODRICH; TAMASSIA, 2013), utilizado em protocolos populares, como o *hyper text transfer protocol secured* (HTTPS), ou protocolo de transferência segura de hipertexto, para acessar *sites* dados como seguros (COMER, 2016; GOODRICH; TAMASSIA, 2013; TANENBAUM; VAN STEEN, 2007). Nomeado pelas iniciais de seus criadores (RIVEST; SHAMIR; ADLEMAN, 1978), o RSA tem como princípio que não há nenhum método eficaz para achar fatores primos (GOODRICH; TAMASSIA, 2013). Com base no conceito de chave pública e privada (Figura 1), que são geradas a partir de números primos muito grandes (milhares de casas decimais), a técnica se mostra eficaz até o momento, devido à complexidade de buscar o padrão ou chegar ao mesmo resultado para gerar essas chaves. Apesar de sua eficiência, a complexidade do RSA para criptografar todos os dados pode trazer um grande problema computacional.

Existem técnicas que combinam o uso de RSA e DES, mas é importante compreender que todas elas são baseadas em algoritmos que determinam como as chaves criptográficas devem se comportar. Além disso, técnicas de ataque, como a de “força bruta”, consomem recursos demais para conseguir quebrar as técnicas criptográficas, fazendo a maioria dos atacantes desistir.



Fique atento

Técnicas de controle de acesso por meio de bases de usuários e uso de *firewall* (COULOURIS *et al.*, 2013) também são importantes para a segurança de um sistema. Como são itens relacionados a redes de computadores, leia o capítulo Sistemas Distribuídos, do livro *Sistemas distribuídos: conceitos e projeto* de Coulouris *et al.* (2013).

3 Assinaturas digitais

O último ponto a ser discutido são os canais seguros, como definido por Tanenbaum e Van Steen (2007, p. 240), “Um canal seguro protege remetentes e receptores contra a interceptação, modificação e invenção de mensagens. Não protege necessariamente contra interrupção [...]”. O autor também ressalta que não é possível discutir sobre protocolos de autenticação sem ter garantias de autenticidade e integridade das mensagens trocadas entre os dispositivos.

Para facilitar a troca de mensagens em um canal seguro, é comum definir uma chave de sessão, que será utilizada para criptografia de comunicação entre dois pontos e que existe apenas enquanto o canal for válido. Quando o canal deixa de existir, a chave de sessão também, ou seja, o mecanismo de criptografia e descryptografia desaparece. Isso garante que sejam trocadas apenas mensagens entre os pares que confirmaram que o canal é seguro.

Para ser seguro, um canal tem de ter essencialmente dois itens (TANENBAUM; VAN STEEN, 2007):

- autenticidade — define que os participantes de uma determinada sessão, os quais, porventura, irão trocar mensagens entre si, de fato, são quem dizem ser. É importante para garantir que a confidencialidade de integridade das mensagens não seja comprometida, nesse caso, a autenticidade tem a ver com a garantia dos nós e das pessoas envolvidas;
- integridade e confidencialidade — os princípios aplicados às mensagens trocadas entre os pares de um canal seguro definem que elas chegarão intactas ao seu receptor (não considerando questões de transporte de mensagem, focando apenas na abstração de alto nível do que é a mensagem no sistema distribuído) e que não poderão serem lidas por nenhum outro usuário do sistema.

Esses princípios, complementares entre si, garantem que o canal, depois de firmado entre os pares, fique seguro pelo maior tempo possível.

Para que a mensagem esteja segura entre os pontos A e B e os princípios da integridade e confidencialidade no sistema distribuído (ou qualquer outro, pois são princípios que se repetem em diversos meios computacionais) sejam garantidos, é interessante que, tanto A como B, tenham assinaturas digitais. Como definido por Coulouris *et al.* (2013, p. 487), “[...] simula a função das assinaturas convencionais, verificando com um outro elemento se uma mensagem, ou um documento, é uma cópia inalterada do que foi produzido pelo signatário [...]”. A forma mais simples de usar uma assinatura digital é por meio de certificados digitais. Um certificado digital é um documento eletrônico contendo uma declaração, emitida por uma unidade certificadora sobre a autenticidade de quem o porta (COULOURIS *et al.*, 2013).



Saiba mais

Você sabia que o Brasil tem uma unidade certificadora central? O ICP-Brasil é um órgão do governo que define como as unidades certificadoras devem atuar, os documentos necessários e outros requisitos para que haja padronização do processo de certificação digital. Para conhecer todo o processo de requisitos, procure na internet pelo documento “Assinaturas digitais na ICP-Brasil”.

Diversos elementos táticos são utilizados para conter um ataque. Para compreender melhor todos eles, leia *Resposta a incidentes de segurança em computadores: planos para proteção de informação em risco*, de McCarthy (2014), principalmente os capítulos 1 e 2, que tratam da necessidade de um governo ter um programa de resposta às ameaças cibernéticas.

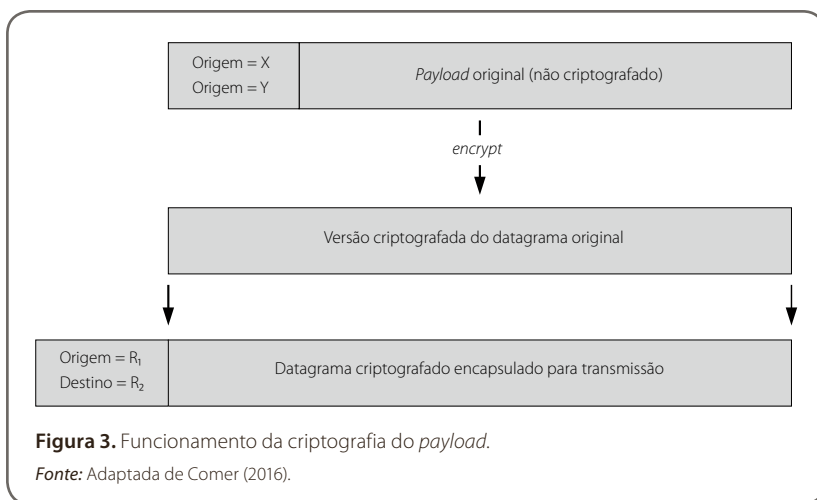
Os certificados digitais podem garantir os aspectos de confidencialidade e integridade por meio das assinaturas digitais. Se todos os dados passarem por um processo de assinatura digital, o resultado é uma comunicação entre dois pontos sempre criptografada e autêntica (os demais pilares vêm em outros pontos da estrutura do sistema distribuído). Como definido por Comer (2016, p. 449), “Políticas de autorização não têm sentido sem um mecanismo de autenticação que possa verificar inequivocamente a identidade de um remetente [...]”.

Tunelamento *versus* criptografia

Conforme abordado anteriormente, pode existir um túnel (canal seguro de comunicação entre emissor e receptor) ou criptografia de dados (RSA, DSE, entre diversos outros), porém, há um modelo mais eficaz na segurança de um sistema distribuído.

Criptografia é muito útil para manter seguro o conteúdo de um pacote de dados (também chamado de *payload* na definição de pacotes de redes), contudo, mantém questões de transmissão intactas. Por exemplo, sempre que você transmite informações para sua família, os dados podem ser criptografados, mas as informações que levam o pacote serão sempre as mesmas. Esse fato pode ser considerado como uma vulnerabilidade a ser explorada por um atacante. Nesse contexto, entram as questões de túnel ou canal seguro, para que não apenas os dados sejam criptografados, mas toda a conexão.

A Figura 3 exibe essa relação argumentada por Comer (2016). Nela, é possível visualizar que todo conteúdo original está criptografado, e o pacote completo passa por um processo de criptografia. Deve-se considerar que todo esse processo adiciona *delay* (tempo decorrente para que um pacote possa ser transmitido e recebido pelo outro dispositivo) na transmissão e na recepção de dados, fazendo toda a técnica ser inviável, dependendo do volume de transmissão.

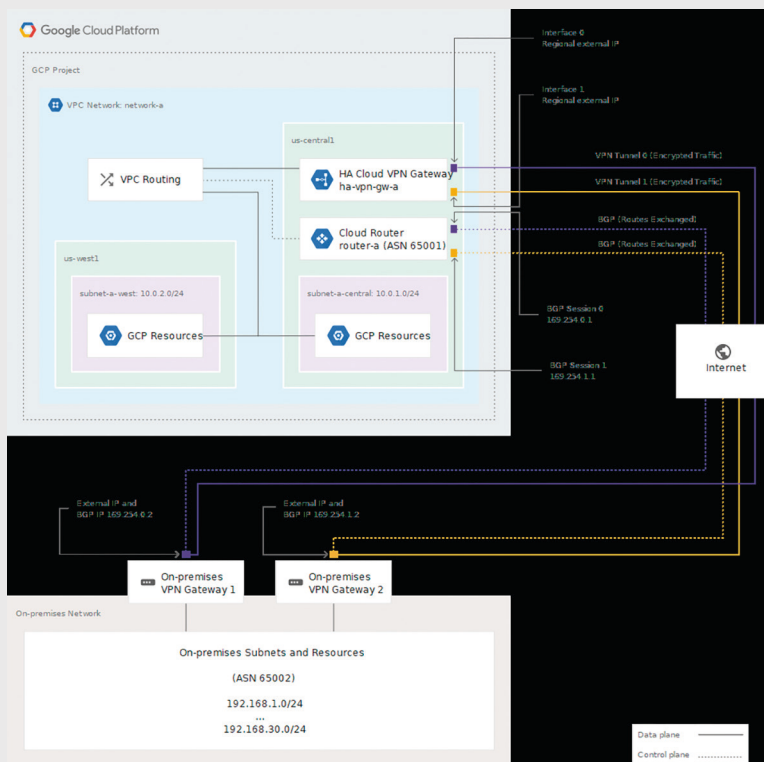


Exemplo

Em um mundo de sistemas distribuídos, é comum que diversos serviços rodem em diferentes empresas, e como criar conexões seguras entre esses serviços é uma questão pertinente.

O exemplo mais simples é o uso de *virtual private network* (VPN), ou rede virtual privada, entre os serviços. Uma VPN é um circuito virtual privado e criptografado que cria um túnel na infraestrutura já consolidada da internet. Esse túnel sempre ligará diferentes dispositivos computacionais, em diversos locais do mundo que precisam trocar informações. No Brasil, houve um caso de bloqueio de um aplicativo de conversa instantânea, em que a determinação judicial dizia que os servidores não poderiam funcionar, mas o aplicativo é utilizado em outros países também. A solução foi utilizar uma VPN que criasse um túnel, cuja entrada fosse no Brasil e a saída em qualquer outro lugar do mundo, possibilitando o acesso ao aplicativo normalmente.

A imagem a seguir mostra como o serviço de VPN do Google *Google Cloud Platform* (GCP), a nuvem do Google, permite a conexão com outros serviços de nuvem.



Fonte: Adaptada de Google Cloud (2020).

Perceba que as linhas azuis e douradas fazem o tráfego de dados de forma encip-tada, não sendo possível que outro dispositivo na internet possa compreender o que se passa naquela conexão. Obviamente, além dessas conexões, o Google cria uma série de regras, *firewalls* e permissões que devem ser obedecidas ou manualmente modificadas para que essa conexão seja possível.



Referências

COMER, D. E. *Redes de computadores e internet*. 6. ed. Porto Alegre: Bookman, 2016.

COULOURIS, G. *et al. Sistemas distribuídos: conceitos e projeto*. 5. ed. Porto Alegre: Bookman, 2013.

GOODRICH, M. T.; TAMASSIA, R. *Introdução à segurança de computadores*. Porto Alegre: Bookman, 2013.

GOOGLE CLOUD. *Visão geral do Cloud VPN*. 2020. Disponível em: <https://cloud.google.com/vpn/docs/concepts/overview>. Acesso em: 03 jun. 2020.

MCCARTHY, N. K. *Resposta a incidentes de segurança em computadores: planos para proteção de informação em risco*. Porto Alegre: Bookman, 2014.

RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, [s. l.], v. 21, n. 2, p. 120–126, 1978.

TANENBAUM, A. S.; VAN STEEN, M. *Sistemas distribuídos: princípios e paradigmas*. 2. ed. São Paulo: Pearson Prentice Hall, 2007.



Fique atento

Os *links* para *sites* da *web* fornecidos neste capítulo foram todos testados, e seu funcionamento foi comprovado no momento da publicação do material. No entanto, a rede é extremamente dinâmica; suas páginas estão constantemente mudando de local e conteúdo. Assim, os editores declaram não ter qualquer responsabilidade sobre qualidade, precisão ou integridade das informações referidas em tais *links*.

Assinatura digital

Objetivos de aprendizagem

Ao final deste texto, você deve apresentar os seguintes aprendizados:

- Compreender o que é uma assinatura digital.
- Identificar os tipos de chaves criptográficas.
- Reconhecer a cadeia hierárquica de confiança que viabiliza a emissão de assinaturas digitais.

Introdução

As pessoas e as empresas passaram a utilizar a Internet para trocar todo tipo de informações, inclusive financeiras, mas o fato é que a rede mundial não oferece a segurança necessária para que as operações virtuais sejam feitas com tranquilidade.

Nesse sentido, a assinatura digital é uma forma de autenticar informações digitais contidas em documentos eletrônicos, garantindo que o indivíduo que está assinando virtualmente o documento, é quem ele realmente diz ser.

Neste capítulo, você vai estudar o conceito de assinatura digital, os tipos de chaves criptográficas e conhecer a cadeia hierárquica de confiança que viabiliza a emissão de assinaturas digitais.

O que é assinatura digital

Com a expansão da informática, tanto para pessoas físicas quanto para empresas, grande parte dos arquivos e documentos transita ou pela Internet, ou por outro meio digital. As empresas passaram a utilizar a Internet para efetivar seus negócios, visando maior agilidade em seus processos e aumento dos lucros obtidos. As pessoas passaram a executar virtualmente as atividades que desempenhavam apenas fisicamente, incluindo assinatura de contratos, declaração de imposto de renda e pagamento de faturas. Apesar da facilidade oferecida pela Internet, a privacidade, o sigilo e a segurança ficaram ameaçados.

Em vista disso, a assinatura digital configura uma forma de conferir segurança, autenticidade e integridade para os documentos eletrônicos. Ela surgiu como uma maneira de provar a veracidade das informações contidas nos documentos digitais, em substituição às assinaturas convencionais que validam documentos em papel. O termo assinatura não foi escolhido em vão: a intenção é remeter à assinatura feita à mão em documentos confeccionados em papel.



Fique atento

Uma assinatura digital não é a mesma coisa que uma assinatura eletrônica. A assinatura eletrônica envolve qualquer forma de identificação do remetente de uma mensagem emitida digitalmente, sem que haja necessidade de regulamentação ou meios para tornar a assinatura confiável. Como exemplo, pode-se citar a identificação do remetente de uma mensagem de correio eletrônico.

Uma assinatura digital é uma técnica ou ferramenta aceita pelo governo, pelo judiciário e pelas empresas, que possibilita que um usuário faça a reprodução de sua assinatura em documentos digitais, sem que a necessidade de utilizar papel na operação. A utilização da assinatura digital, principalmente pelas empresas, traz uma grande economia no volume de papel gasto, além de economizar espaço de armazenamento e em despesas com correio.

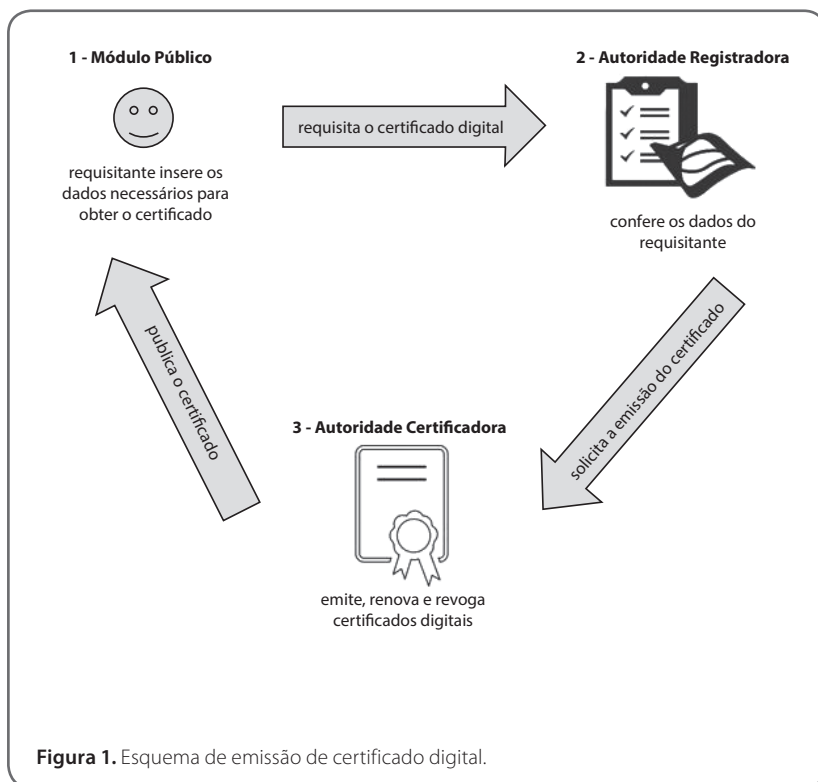
A assinatura digital é uma ferramenta extremamente segura, pois utiliza criptografia e vincula, em todos os documentos assinados, um certificado digital que é obtido previamente e que serve para comprovar a sua autenticidade. Em outras palavras, a assinatura convencional do titular é substituída por uma assinatura digital, que vem com um certificado e uma chave privada exclusiva do titular, o que lhe confere veracidade. Esse certificado é assinado por uma das inúmeras autoridades certificadoras, entidades credenciadas em que todos confiam. Para obter uma assinatura digital, é preciso fazer a solicitação para uma das Autoridades Certificadoras.

Foi a partir de 2001, com a criação da Infraestrutura de Chaves Públicas Brasileiras (ICP-Brasil) que os documentos digitais puderam ser assinados digitalmente, substituindo totalmente o uso do papel, e com validade, inclusive jurídica, em todo o Brasil (BRASIL, 2018). A ICP-Brasil configura um sistema de serviços, políticas e recursos que dá suporte para a utilização de criptografia

de chave pública, possibilitando fazer a autenticação das partes envolvidas em uma transação digital. Ela fornece as ferramentas necessárias para gerenciar os certificados digitais e as chaves públicas, formando uma cadeia hierárquica de confiança que viabiliza a emissão dos certificados digitais para a identificação virtual de alguém que está assinando um documento virtualmente.

A ICP-Brasil é responsável pela regulamentação das práticas e dos procedimentos de emissão de certificados digitais, além de outros serviços digitais associados a eles. Um processo normal de emissão de certificado digital (Figura 1), ou seja, que possibilita a veracidade da assinatura digital, envolve os seguintes elementos (BALDAM, 2016):

- **Módulo Público** — é um portal de serviços, onde o usuário final solicita o certificado digital ou faz a instalação do certificado digital. Por meio do módulo público é possível também acompanhar, pela interface de status do processo, como está o andamento da emissão do certificado digital.
- **Autoridade certificadora (AC)** — é a entidade responsável por emitir, gerar, renovar e revogar os certificados digitais. Também é responsável por distribuir as chaves públicas, emitir a Lista de Certificados Revogados (LCR) e manter as regras de publicação dos certificados digitais. Uma autoridade certificadora pode ser uma empresa, uma organização, um indivíduo público, ou privado. É essa entidade que recebe a requisição do certificado digital (assinada pela autoridade de registro), confere a assinatura digital da autoridade de registro e faz a emissão do certificado digital que será conferido ao usuário final. A forma de funcionamento de uma AC vai determinar quais os tipos de certificado digital que ela é capaz de emitir, e essa informação está descrita em um documento chamado Declaração de Práticas de Certificação (DPC).
- **Autoridade de registro (AR)** — é a entidade que estabelece uma interface entre uma AC e o usuário. É a autoridade de registro que confere as informações do usuário e faz o envio da requisição do certificado para a AC. Essa autoridade é muito importante, já que o nível de confiança atribuído ao certificado está diretamente ligado à qualidade do processo de conferência dessas informações. Uma AC necessariamente vai confiar nas informações passadas por uma AR, e o certificado vai ser emitido sem a necessidade de nenhum outro tipo de verificação nas informações. Por isso a confiança é necessária, a fim de garantir a confiabilidade durante todo o processo.



A assinatura digital permite que um documento digital tenha a mesma validade, inclusive jurídica, de um documento assinado em cartório, por exemplo. A assinatura digital é utilizada para validar muitos documentos e operações que são feitas virtualmente, como a entrega da declaração de imposto de renda e a assinatura de contratos. Uma assinatura digital prova com a máxima certeza que a mensagem recebida pelo destinatário teve origem no remetente que diz ter enviado. Para ser tão segura, uma assinatura digital precisa ter as seguintes características (NAKAMURA; GEUS, 2007):

- **Autenticidade** — o destinatário da mensagem pode confirmar com certeza que a assinatura foi emitida pelo remetente.
- **Integridade** — a certeza de que a mensagem trafegou sem nenhuma alteração do remetente até o destinatário, pois do contrário a assinatura não tem validade.
- **Irretratabilidade** — o remetente não pode negar que a mensagem é autêntica.

Uma assinatura digital é, atualmente, a maneira mais avançada, segura e confiável de fazer uma assinatura eletrônica e substituir a assinatura em papel. Desde que seja emitida pelas autoridades corretas, ela cumpre todas as exigências da legislação a respeito disso.

Tipos de chaves criptográficas

Existem dois tipos de chaves criptográficas para a assinatura digital: a criptografia simétrica e a assimétrica.



Fique atento

A criptografia envolve a aplicação de um algoritmo de codificação em dados que precisam ficar incompreensíveis e ininteligíveis para pessoas que não estão participando de uma transação específica.

Já a descryptografia consiste na aplicação de um algoritmo para tornar a mensagem legível novamente, por um indivíduo que saiba como descryptografar os dados.

Criptografia simétrica

A criptografia simétrica tem fundamento em algoritmos que dependem de uma chave única, que é chamada de chave secreta e utilizada no processo de codificação e decodificação da mensagem, como exposto na Figura 2. Para assegurar a integridade da mensagem transmitida é fundamental que somente o remetente e o destinatário da mensagem conheçam a chave. A criptografia simétrica utiliza a mesma chave para criptografar e descryptografar os dados, logo, o algoritmo utilizado por ela é mais simples e o processo de criptografia é bem mais rápido (SILVEIRA, 2006).

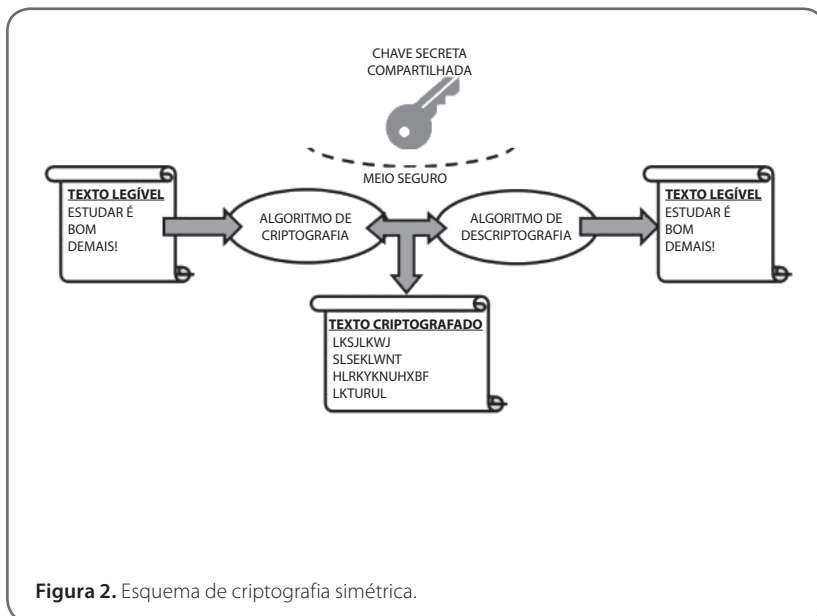


Figura 2. Esquema de criptografia simétrica.

A operação de um algoritmo de chave simétrica é mais simples porque existe apenas uma chave envolvida na comunicação. Essa chave representa um segredo que é compartilhado entre todos os envolvidos para que um canal de comunicação minimamente confidencial possa ser estabelecido e mantido, ou seja, esse tipo de criptografia exige que seja utilizado um canal protegido para que a troca de chave seja feita, o que torna esse tipo de criptografia menos utilizado.

O princípio básico da criptografia simétrica é que apenas uma chave é usada pelos envolvidos na troca de mensagens e ela é conhecida apenas por eles. Isso, porém, é praticamente impossível de ser assegurado, já que existe uma facilidade muito grande de ataque e interceptação da troca de mensagens. Esse é o maior problema da criptografia simétrica: a obrigatoriedade do compartilhamento da chave secreta com todos os indivíduos que precisam ler e entender a mensagem, o que possibilita a alteração de partes da mensagem por qualquer um deles.

Outro incômodo com a utilização da criptografia simétrica diz respeito aos gastos com o uso de canais seguros e com a distribuição de chaves, o que torna possível sua utilização somente por quem pode pagar por isso, como governos e grandes instituições bancárias. O gerenciamento da chave secreta também é uma dificuldade do uso desse tipo de criptografia, pois é uma atividade que envolve escolher, distribuir e armazenar as chaves sem erro e sem perda, de

uma maneira que sejam alteradas com frequência e mantidas da forma mais segura possível durante a distribuição e a efetivação da transação.

Criptografia assimétrica

A criptografia assimétrica tem como fundamento a utilização de um par de chaves diferentes entre si, mas que mantêm um relacionamento matemático, o que permite que a mensagem criptografada por uma chave seja descriptografada somente pela outra chave do mesmo par (MARTINI, 2008). As duas chaves necessárias para a criptografia assimétrica são chamadas de chave pública e chave privada, e funcionam como mostrado na Figura 3. A chave pública pode ser de conhecimento do público em geral, mas a chave privada deve ser de conhecimento apenas do seu titular.

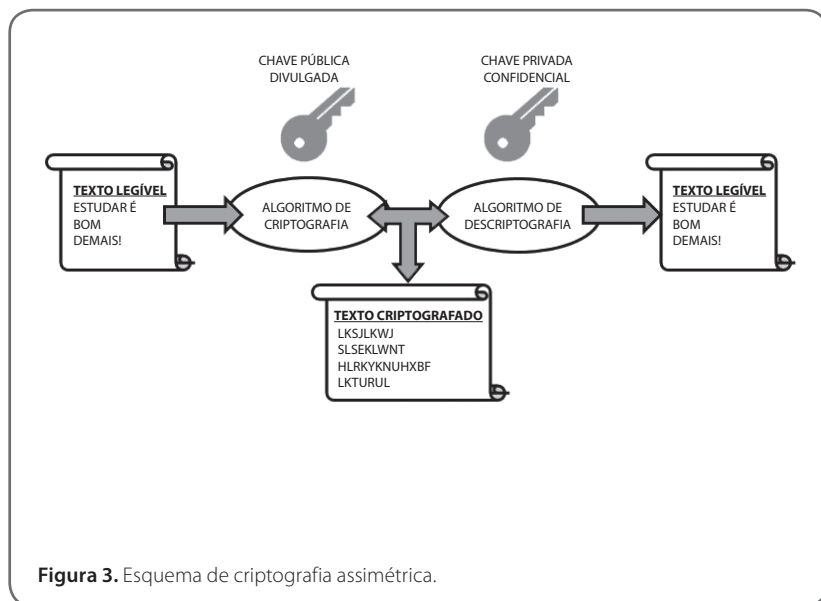


Figura 3. Esquema de criptografia assimétrica.

A obrigatoriedade de compartilhamento da chave secreta única e a utilização de apenas uma chave (características da criptografia simétrica) são resolvidas pela criptografia assimétrica, visto que ela utiliza duas chaves, uma para criptografar e outra para descriptografar. O algoritmo utilizado é mais complexo e por isso o processo de criptografia é mais lento, mas em compensação é bem mais seguro.

Nesse tipo de criptografia, somente uma das partes envolvidas na transação possui a chave privada, que é mantida em segredo e é praticamente impossível deduzi-la. A chave pública é disponibilizada para todas as outras partes envolvidas e, dessa forma, qualquer indivíduo pode criptografar dados. Por outro lado, as mensagens que forem criptografadas pela chave pública só poderão ser descriptografadas pela chave privada, o que oferece segurança e confiabilidade para a operação de comunicação.

A cadeia hierárquica de confiança

Apesar de a ideia das assinaturas digitais ser antiga, no Brasil ela foi implementada por meio da Medida Provisória nº. 2.200–2/2001, que instituiu a ICP-Brasil (BRASIL, 2001). O propósito da ICP-Brasil é explicado logo em seu artigo primeiro:

Art. 1º Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras (BRASIL, 2001, documento on-line).

Essa medida provisória, que permanece em vigor, deixa claro que todos os documentos digitais com certificado emitido pela ICP-Brasil possuem validade em todos os segmentos, inclusive no jurídico. Entretanto, a Medida Provisória nº. 2.002–2/2001 também libera a comprovação de autenticidade por outros meios de comprovação de titularidade, mesmo os não emitidos pela ICP-Brasil, desde que ambas as partes envolvidas na transação aceitem esse outro meio como válido. Em outras palavras, a ICP-Brasil é a autoridade brasileira oficial que informa e gerencia as técnicas disponíveis para gerar documentos digitais válidos. Porém, ela não é a única, nada impede a existência de outras entidades e outros meios de validação de documentos. Ao longo do texto da Medida Provisória, fica estabelecido que a ICP-Brasil será formada tanto por ACs, quanto por ARs, ou seja, uma entidade não é mais importante ou principal do que a outra. As entidades são escolhidas pelos requisitantes de acordo com a funcionalidade requerida para o certificado digital em questão.

A ICP-Brasil é responsável pelo conjunto de regras e padrões que permitem a compatibilidade entre os vários tipos de certificados digitais existentes, fornecendo um nível de segurança compatível com os melhores padrões

disponíveis atualmente (MARTINI, 2008). Existe um rígido controle, feito por meio de auditoria, em todas as entidades que participam da ICP-Brasil. Esse controle é fundamental porque aumenta a confiabilidade depositada nos padrões seguidos. Atualmente, a ICP-Brasil é formada basicamente pelas seguintes entidades (BRASIL, 2018):

- **Autoridade certificadora (AC)** — essa entidade pode ser pública ou privada, e é subordinada hierarquicamente à ICP-Brasil. Seu papel é verificar se o titular do certificado tem a chave privada correspondente à chave pública que faz parte daquele certificado. A AC faz a criação e a assinatura digital do certificado do usuário. O certificado emitido pela AC representa a declaração de identidade do titular, que possui um par único de chaves pública e privada. Essa entidade também emite uma LCR e mantém os registros de suas operações.
- **Autoridade de registro (AR)** — essa entidade faz o intermédio entre o requisitante do certificado digital e a AC. Ela é vinculada a uma AC e tem como responsabilidade receber, validar e encaminhar as solicitações de emissão ou revogação de certificados digitais, além de identificar de forma presencial os requisitantes. Essa entidade também tem que manter um registro de todas as suas operações e pode estar localizada fisicamente em uma AC, ou ser uma entidade de registro que opera remotamente.
- **AC–Raiz** — a AC–Raiz é a primeira da cadeia de certificação. Sua atribuição é executar as políticas de certificados e as normas técnicas e operacionais que são aprovadas pelo comitê gestor da ICP-Brasil, além de verificar se as ACs estão atuando conforme as diretrizes e normas técnicas estabelecidas pelo comitê. Suas atividades envolvem a emissão, a expedição, a distribuição, a revogação e o gerenciamento dos certificados das ACs de nível imediatamente subsequente ao seu nível. Essa entidade também faz a emissão de uma LCR, e fiscaliza e audita ACs, ARs e demais prestadores de serviço que são habilitados pela ICP-Brasil.
- **Autoridade certificadora do tempo (ACT)** — essa entidade é responsável pelo fornecimento do Carimbo do Tempo, um conjunto de atributos fornecidos pela parte confiável do tempo, que confere prova de sua existência em determinado período, sendo associado a uma assinatura digital. Resumindo, quando um documento é produzido, seu conteúdo é criptografado e recebe atributos (ano, mês, dia, hora, minuto, segundo), e em seguida é atestado com uma assinatura, realizada por meio de

certificado digital que comprova sua autenticidade. A ACT atesta, então, a questão de tempo de uma transação e também o seu conteúdo.

- **Prestador de serviço de suporte (PSS)** — é a entidade que executa as atividades descritas na política do certificado e na DPC da AC à qual está vinculada diretamente, ou por intermédio da AR.
- **Prestador de serviço biométrico (PSBio)** — é a entidade que tem capacidade técnica para realizar a identificação biométrica, possibilitando um registro único nos bancos de dados e sistemas de dados biométricos de toda a ICP-Brasil. Ela realiza a verificação biométrica do requisitante de um certificado digital e faz a comparação da biometria, que tem característica única, de acordo com padrões internacionais de utilização.

São muitas as ACs credenciadas pela ICP-Brasil, não sendo possível eleger uma mais importante, pois a escolha da AC pelo requisitante vai depender do tipo de certificado digital pretendido por ele. As ACs que se destacam como órgãos do governo ou grandes entidades são (BRASIL, 2018):

- **Serviço Federal de Processamento de Dados (Serpro)** — primeira AC credenciada pela ICP-Brasil.



Link

Para saber como se obtém um certificado digital através da Serpro, acesse o *link* ou código a seguir:



<https://goo.gl/z4gZjX>

- **Caixa Econômica Federal** — única instituição financeira brasileira credenciada como AC da ICP-Brasil.



Link

Para saber como se obter um certificado digital através da Caixa Econômica Federal, acesse o *link* ou código a seguir:



<https://goo.gl/wMwuKY>

- **Serasa Experian** — AC que pertence ao setor privado. Ela fornece a segurança dos certificados digitais para quase a totalidade dos grupos financeiros que participam do Sistema de Pagamentos Brasileiro.
- **Certisign** — AC que tem foco duplo no segmento da certificação digital pois, além de viabilizar o fornecimento de uma ferramenta tecnológica, ainda desenvolve soluções para utilização exclusiva com certificados digitais emitidos pela ICP-Brasil.
- **Casa da Moeda do Brasil** — essa AC é uma das mais antigas instituições públicas brasileiras. A Casa da Moeda modernizou sua estrutura produtiva e administrativa, habilitando-se a prestar atendimento ao mercado de segurança na era da tecnologia.



Referências

BALDAM, R. *Gerenciamento de conteúdo empresarial*. Rio de Janeiro: Elsevier, 2016.

BRASIL. Instituto Nacional de Tecnologia da Informação. *ICP-Brasil*. 2018. Disponível em: <<http://www.iti.gov.br/icp-brasil>>. Acesso em: 1 ago. 2018.

BRASIL. *Medida Provisória nº. 2.200-2, de 24 de agosto de 2001*. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Brasília, DF, 2001. Disponível em: <http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm>. Acesso em: 1 ago. 2018

MARTINI, R. S. *Tecnologia e cidadania digital: tecnologia, sociedade e segurança*. Rio de Janeiro: Brasport, 2008.

NAKAMURA, E. T.; GEUS, P. L. *Segurança de redes em ambientes cooperativos*. São Paulo: Novatec, 2007.

SILVEIRA, S. A. Criptografia assimétrica...você ainda vai precisar dela. *Revista Eletrônica A REDE*, São Paulo, nº. 10, p. 32-33, jan. 2006.

Autenticação de meios eletrônicos

Objetivos de aprendizagem

Ao final deste texto, você deve apresentar os seguintes aprendizados:

- Definir as espécies de registro em meio eletrônico.
- Descrever os efeitos do registro de um título ou documento.
- Examinar o embasamento legal para a digitalização registrada dos documentos.

Introdução

A sociedade contemporânea vive a era digital e, nesse tempo, é necessária a adequação dos serviços de registros de títulos e documentos para a autenticação por meios eletrônicos. O registro eletrônico tem como objetivo melhorar os serviços prestados pelo registro de títulos e documentos (RTD), promovendo agilidade e eficácia, bem como a redução de custos e burocracias para se obter documentos, mediante a solicitação por meio eletrônico.

Neste capítulo, você vai ler sobre as espécies de registro por meio eletrônico e seus efeitos. Para tanto, você verá a abordagem do arcabouço jurídico legal que permite dar autenticidade aos documentos eletrônicos.

1 Espécies de registro em meio eletrônico

A Lei nº. 12.682, de 9 de julho de 2012 (BRASIL, 2012, documento *on-line*), em seu art. 2-A, autoriza “[...] o armazenamento, em meio eletrônico, óptico ou equivalente, de documentos públicos ou privados, compostos por dados ou por imagens, observado o disposto nesta Lei, nas legislações específicas e no regulamento”.

A Lei nº. 13.874, de 20 de setembro de 2019, além de alterar a Lei nº. 12.682/2012, fez alterações em diversas legislações para incluir o meio eletrônico em seus documentos (BRASIL, 2019a). Nesse sentido, o art. 1º, § 3º, da Lei de Registros Públicos foi alterada para incluir a possibilidade de escrituração, publicização e conservação dos registros públicos ocorrerem de forma eletrônica, passando a prever que: “[...] os registros poderão ser escriturados, publicitados e conservados em meio eletrônico, obedecidos os padrões tecnológicos estabelecidos em regulamento” (BRASIL, 1973, documento *on-line*).

Na mesma linha, a Lei nº. 8.934, de 18 de novembro de 1994 (BRASIL, 1994a), passou a vigorar, no art. 65-A, que seus atos de constituição, alteração, transformação, incorporação, fusão, cisão, dissolução e extinção de registro de empresários e de pessoas jurídicas poderão ser realizados também por meio de sistema eletrônico criado e mantido pela Administração Pública Federal.

Na seara trabalhista, a lei alterou o art. 29 da Consolidação das Leis do Trabalho (CLT), passando a permitir que os registros eletrônicos gerados pelo empregador nos sistemas informatizados da Carteira de Trabalho e Previdência Social (CTPS) em meio digital possam equivaler às anotações físicas da CTPS, bem como o ponto pode ser realizado por registro eletrônico, em conformidade com a nova redação do art. 74 da CLT (BRASIL, 2019a). Por fim, a lei estabelece a autenticidade aos documentos particulares digitalizados, desde que assinados digitalmente e de comum acordo entre as partes, por força do art. 18, I, da Lei nº. 13.874/2019 (BRASIL, 2019a).

A Lei nº. 11.977, de 7 de julho de 2009 (BRASIL, 2009), prevê nos arts. 37 a 45 que todos os serviços registrares, previstos pela lei de serviços públicos, devem instituir os registros eletrônicos, incluindo os atos notariais e as certidões.

A Lei nº. 12.965, de 23 de abril de 2014 (BRASIL, 2014), nos incisos II e III do art. 3º e no art. 11, dispõe sobre os princípios, a proteção aos registros, os dados pessoais e as comunicações privadas.

O Provimento nº. 48, de 16 de março de 2016, do Conselho Nacional de Justiça (CNJ) (BRASIL, 2016), estabelece as diretrizes gerais para o sistema de registro eletrônico de títulos e documentos e civil de pessoas jurídicas. Em síntese, o sistema de registro eletrônico de títulos e documentos e civil de pessoas jurídicas deverá ser implantado e integrado por todos os oficiais de RTD e civil de pessoas jurídicas de cada Estado, do Distrito Federal e dos territórios. Somente o ofício de RTD e civil de pessoas jurídicas competente será o único responsável pelo processamento e atendimento.

Mais recentemente, o CNJ editou o Provimento nº. 89, de 18 de dezembro de 2019 (BRASIL, 2019b), que regulamentou o registro eletrônico de imó-

veis, que passou a vigorar a partir de 1º de janeiro de 2020 — o Sistema de Registro Eletrônico de Imóveis (SREI), o Serviço de Atendimento Eletrônico Compartilhado e o acesso da Administração Pública Federal às informações do SREI — e estabeleceu diretrizes para o estatuto do Operador Nacional do Sistema de Registro Eletrônico e foi concebido para ser um repositório eletrônico de dados relativos aos serviços de registro imobiliário de caráter nacional, com a finalidade de integrar as unidades registras e suas bases de dados, sob o acompanhamento, a regulação-normativa e a fiscalização da Corregedoria Nacional. Inúmeros são os exemplos de espécies registráveis eletronicamente, como:

- acordos;
- atas condominiais;
- boletim de ocorrência;
- cédulas e cessões de créditos;
- contratos de todas as espécies;
- doação;
- faturas;
- instrumentos de transação;
- laudos;
- notificações;
- ofícios;
- pactos;
- revogações;
- testamentos.

Todas as espécies têm suas respectivas certidões, que podem ser obtidas na forma eletrônica, com assinatura digital, que assegura plenamente a sua procedência e a responsabilidade de quem a emitiu, ou, na forma física, impressa em papel. Ambas têm o mesmo valor do documento original, para todos os fins e efeitos legais, em razão da fé pública do oficial registrador (Lei nº. 8.935, de 18 de novembro de 1994, art. 3º) (BRASIL, 1994b).



Saiba mais

Para explorar a lista de exemplos de documentos registráveis em títulos e documentos, digite “cartoriortdcampinas” no seu mecanismo de busca.

2 Efeitos do registro de título ou documento

Em resposta à consulta formulada sobre registro em meio eletrônico ao 2º RTD — Registro de Imóveis de Osasco —, os efeitos do registro de um título ou documento no RTD são:

- a. autenticação da data: o registro indica a data em que foi preservado o documento.
- b. publicidade do conteúdo do registro: qualquer terceiro interessado poderá requisitar uma certidão do documento registrado;
- c. perpetuação do documento registrado: o RTD deverá guardar para sempre uma cópia do documento, em qualquer mídia: papel, microfilme ou digital (MP 2.200/01).
- d. eficácia contra terceiros: uma espécie de publicidade qualificada para os contratos do artigo 129 da Lei 6.015/73 — a Lei de Registros Públicos, que tratam principalmente de direito real sobre bem móvel, que significa que se o registro foi feito nos RTDs do domicílio do credor e devedor está estabelecida a má-fé de eventual terceiro adquirente da coisa, que não poderá se opor ao direito do credor original.

Todo e qualquer registro em RTD conta com os três primeiros efeitos acima. Por isso, não bastasse artigo expresso da lei neste sentido, a certidão do registro feito em RTD tem efeito de original. Afinal, o documento original está preservado, de forma pública e com data autenticada para sempre (PINHO, [2020?], documento *on-line*).

Sobre os efeitos do registro de um título ou documento no RTD, não basta que um documento seja digitalizado, é necessário conferir autenticidade aos documentos eletrônicos originados pela digitalização e conservar esses arquivos eletrônicos de forma segura, tornando-os disponíveis a qualquer tempo e de qualquer lugar.

É relevante, ainda, destacar que o documento é emitido por um notório ou registrador com fé pública, sendo, portanto, realizada a emissão de um documento autêntico, presumindo-se verdadeiro, por força do art. 374, do Código

de Processo Civil de 2015 (Lei nº. 13.105, de 16 de março de 2015) (BRASIL, 2015), que somente é extinta por comprovação de falsidade, prevista no art. 430 do mesmo diploma legal.

Sobre a publicidade, segundo Rodrigues (2007, p. 5), existem vários atos e fatos da vida civil e jurídica que devem ser públicos, como:

É obrigatória por exigência legal nos nascimentos (arts. 50 e 52, LRP), óbitos (arts. 77 e 79, LRP), registros e averbações relativos a imóveis (art. 167, I e II, LRP), etc. Tem natureza constitutiva nas sentenças de emancipação, interdição e ausência (arts. 91, parágrafo único; 93, parágrafo único; e 94, LRP); na existência legal das pessoas jurídicas (art. 119, LRP), para a não-clandestinidade do jornal ou publicação periódica (art. 125, LRP); para aquisição da propriedade imóvel (art. 1.245, CC de 2002), etc. Assegura ainda escolha futura de direito no exercício de opção pela nacionalidade brasileira (art. 32, LRP). Consiste também na obrigatoriedade de prestar informações e fornecer certidões (inteiro teor, resumo e em relatório conforme quesitos), no prazo máximo de cinco dias, mediante solicitação de qualquer pessoa, sem declarar o motivo ou interesse, cabendo ao registrador fornecer nota de entrega autenticada no ato do recebimento do pedido (arts. 16, 19, 20 e seu parágrafo único, LRP), bem como a obrigatoriedade de fazer menção sobre qualquer alteração posterior ao ato cuja certidão é pedida, sob pena de responsabilidade funcional, civil e criminal (art. 21, LRP). Exceções: legitimação, reconhecimento e adoção (arts. 45 e 94 da LRP) — só por ordem judicial.

Sob o efeito da perpetuação do documento registrado, ele advém da segurança jurídica, insculpida constitucionalmente no art. 5º, *caput*, da Constituição Federal (BRASIL, 1988).

No que concerne à eficácia, por ser o ato realizado por um notário ou um registrador que exerce função delegada pública, por força do art. 236 da Constituição Federal (BRASIL, 1988), há presunção de legalidade em relação aos atos que praticam, isto é, presume-se que todos os documentos certificados ou atestados devem ser verdadeiros e, assim, devem estar aptos a produzir efeitos, não somente entre as partes, mas também em relação à oponibilidade contra terceiros. Paiva (2009) acrescenta que os registros públicos possuem três efeitos:

- o constitutivo, posto que, sem o registro, o direito não nasce;
- os comprobatórios, uma vez que o registro prova a existência e a veracidade do ato ao qual se reporta;
- o publicitário, que é o ato registral acessível à ciência de todos.



Saiba mais

Paiva (2009) traz como exemplos dos efeitos dos registros públicos: do constitutivo, a emancipação; do comprobatório, a usucapião; e do publicitário, a adoção judicial.

3 Embasamento legal para a digitalização registrada dos documentos

De acordo com Paiva (2015, documento *on-line*), a definição de registro eletrônico é “[...] ato registral nato digital estruturado assinado digitalmente pelo titular da serventia, seu substituto legal ou escrevente autorizado”, em conformidade com os Padrões de Interoperabilidade de Governo Eletrônico (e-PING) e requisitos da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). O registro eletrônico no Brasil foi introduzido pela Lei nº. 11.977/2009 (BRASIL, 2009, documento *on-line*), nos arts. 37 a 39:

Art. 37 Os serviços de registros públicos de que trata a Lei nº. 6.015, de 31 de dezembro de 1973, observados os prazos e condições previstas em regulamento, instituirão sistema de registro eletrônico.

Art. 38 Os documentos eletrônicos apresentados aos serviços de registros públicos ou por eles expedidos deverão atender aos requisitos da Infra-estrutura de Chaves Públicas Brasileira — ICP e à arquitetura ePING (Padrões de Interoperabilidade de Governo Eletrônico), conforme regulamento.

Parágrafo único. Os serviços de registros públicos disponibilizarão serviços de recepção de títulos e de fornecimento de informações e certidões em meio eletrônico.

Art. 39 Os atos registrais praticados a partir da vigência da Lei nº. 6.015, de 31 de dezembro de 1973, serão inseridos no sistema de registro eletrônico, no prazo de até 5 (cinco) anos a contar da publicação desta Lei.

Parágrafo único. Os atos praticados e os documentos arquivados anteriormente à vigência da Lei nº. 6.015, de 31 de dezembro de 1973, deverão ser inseridos no sistema eletrônico.



Saiba mais

"A Central Nacional de RTD e de Registro Civil de Pessoas Jurídicas (RTDPJ) foi criada pelos próprios oficiais de registro do Brasil por deliberação em assembleia geral realizada em 12 de novembro de 2012. A criação da central visou atender às disposições dos arts. 37 a 39 da Lei nº. 11.977/2009, tendo sido posteriormente normatizada com a edição do Provimento nº. 48/2016 do CNJ. Atualmente, a Central RTDPJ Brasil atua nos 26 Estados brasileiros e no Distrito Federal" (CENTRAL RTDPJBRASIL, 2020, documento *on-line*).

[...]

"É a maior plataforma de registro eletrônico do País. Cabe à central o acompanhamento de todo o processo, desde a solicitação por parte do cliente até a emissão do registro por parte dos cartórios. A plataforma é uma solução tecnológica que permite aos seus usuários economia de tempo, agilidade e conforto no momento de utilizar os serviços oferecidos pelos cartórios. A Central RTDPJ Brasil é vinculada administrativamente ao Instituto de RTD e Pessoas Jurídicas do Brasil (IRTPJ Brasil) e tem suas atividades reguladas pelo CNJ" (CENTRAL RTDPJBRASIL, 2020, documento *on-line*).

No tocante ao embasamento legal do registro eletrônico, a Lei nº. 6.015/1973 (Lei de Registros Públicos) (BRASIL, 1973) trata dos efeitos dos registros no RTD e das atribuições legais dos notários e registradores, como fazer constar no documento registrado o valor cobrado e ainda o valor probante do documento eivado de fé pública e a quem se destina a norma. Outra legislação aplicável aos registros eletrônicos é a Lei nº. 8.935/1994 (Lei de Notários e Registradores) (BRASIL, 1994b), que trata do dever de o oficial do RTD cumprir suas atribuições legais, de dar recibo dos valores recebidos e da possibilidade de o oficial utilizar os processos eletrônicos.

A Medida Provisória nº. 2.200-1, de 27 de julho de 2001 (reeditada pela Medida Provisória nº. 2.200-2, de 24 de agosto de 2001) (BRASIL, 2001), instituiu a ICP-Brasil para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.



Fique atento

A Medida Provisória nº. 2.200-1/2001 (reeditada pela Medida Provisória nº. 2.200-2/2001) (BRASIL, 2001) manteve-se em vigor mesmo após a aprovação da Emenda Constitucional nº. 32, de 11 de setembro de 2001, que determinou o prazo de validade de 60 dias prorrogáveis para que as medidas provisórias se tornassem leis. Isso porque foi publicada um mês antes da data que a Emenda Constitucional entrou em vigor (setembro de 2001).

Além disso, a Lei nº. 12.682/2012 (BRASIL, 2012) dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos.

Da possibilidade de o registro ser eletrônico

O § 3º, art. 1º, da Lei nº. 6.015/1973 (BRASIL, 1973, documento *on-line*) permite que “[...] os registros poderão ser escriturados, publicitados e conservados em meio eletrônico, obedecidos aos padrões tecnológicos estabelecidos em regulamento”.

Do valor probante — autenticidade

O art. 161 da Lei nº. 6.015/1973 (BRASIL, 1973, documento *on-line*): “Art. 161 As certidões do registro integral de títulos terão o mesmo valor probante dos originais, ressalvado o incidente de falsidade destes, oportunamente levantado em juízo.”

O Código Civil brasileiro (Lei nº. 10.406, de 10 de janeiro de 2002) (BRASIL, 2002, documento *on-line*), em seu art. 225, prevê que:

Art. 225 As reproduções fotográficas, cinematográficas, os registros fonográficos e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos ou de coisas fazem prova plena destes, se a parte, contra quem forem exibidos, não lhes impugnar a exatidão.

A Lei nº. 12.682/2012 (BRASIL, 2012, documento *on-line*), em seu art. 2º, § 2º, prevê:

Art. 2º [...]

§ 2º O documento digital e a sua reprodução, em qualquer meio, realizada de acordo com o disposto nesta Lei e na legislação específica, terão o mesmo valor probatório do documento original, para todos os fins de direito, inclusive para atender ao poder fiscalizatório do Estado (Incluído pela Lei nº. 13.874/2019).

O disposto no § 2º da Medida Provisória nº. 2.200-1/2001 (reeditada pela Medida Provisória nº. 2.200-2/2001) (BRASIL, 2001) não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

Da definição do documento eletrônico com a utilização de chave pública

A Medida Provisória nº. 2.200-1/2001 (reeditada pela Medida Provisória nº. 2.200-2/2001) (BRASIL, 2001, documento *on-line*) prevê que o documento eletrônico público e privado deve ser associado a uma assinatura eletrônica, conforme seu art. 1º:

Art. 1º Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira — ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

Da eficiência administrativa por meios tecnológicos

O art. 41 da Lei nº. 8.935/1994 (BRASIL, 1994b) prevê o dever aos notários e registradores, em cumprimento ao princípio constitucional da eficiência administrativa, de adotar todos os meios tecnológicos legais e os processos adequados para melhor prestação do serviço público.

Do armazenamento dos dados

Especialmente no tange à integralidade, esses documentos eletrônicos devem ser armazenados em locais seguros contra o acesso, o uso, a alteração, a reprodução ou a destruição por pessoas não autorizadas, conforme art. 3º da Lei nº. 12.682/2012 (BRASIL, 2012) e art. 6º, do mesmo diploma legal, que dispõe que “[...] os registros públicos originais, ainda que digitalizados, deverão ser preservados de acordo com o disposto na legislação pertinente” (BRASIL, 2012, documento *on-line*). Ainda, a autorização de armazenamento está disposta no art. 2-A, § 1º (BRASIL, 2012).

Da disponibilidade dos dados

A Lei nº. 11.977/2009 (BRASIL, 2009, documento *on-line*) preceitua, em seu art. 41, que:

Art. 41 A partir da implementação do sistema de registro eletrônico de que trata o art. 37, os serviços de registros públicos disponibilizarão ao Poder Judiciário e ao Poder Executivo federal, por meio eletrônico e sem ônus, o acesso às informações constantes de seus bancos de dados, conforme regulamento.



Referências

BRASIL. Conselho Nacional de Justiça. Corregedoria Nacional de Justiça. *Provimento nº 48, de 16 de março de 2016*. Estabelece diretrizes gerais para o sistema de registro eletrônico de títulos e documentos e civil de pessoas jurídicas. Brasília, DF, 2016. Disponível em: https://atos.cnj.jus.br/files//provimento/provimento_48_16032016_16032018112202.pdf. Acesso em: 30 mar. 2020.

BRASIL. Conselho Nacional de Justiça. Corregedoria Nacional de Justiça. *Provimento nº 89, de 18 de dezembro de 2019*. Regulamenta o Código Nacional de Matrículas - CNM, o Sistema de Registro Eletrônico de Imóveis - SREI... Brasília, DF, 2019b. Disponível em: <https://www.cnj.jus.br/wp-content/uploads/2019/12/Provimento-n%C2%BA89.pdf>. Acesso em: 30 mar. 2020.

BRASIL. Presidência da República. Casa Civil. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 30 mar. 2020.

BRASIL. Presidência da República. Casa Civil. *Lei nº. 6.015, de 31 de dezembro de 1973*. Dispõe sobre os registros públicos e dá outras providências. Brasília, DF, 1973. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L6015compilada.htm. Acesso em: 30 mar. 2020.

BRASIL. Presidência da República. Casa Civil. *Lei nº. 8.934, de 18 de novembro de 1994*. Dispõe sobre o Registro Público de Empresas Mercantis e Atividades Afins e dá outras providências. Brasília, DF, 1994a. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L8934.htm. Acesso em: 30 mar. 2020.

BRASIL. Presidência da República. Casa Civil. *Lei nº. 8.935, de 18 de novembro de 1994*. Regulamenta o art. 236 da Constituição Federal, dispondo sobre serviços notariais e de registro (Lei dos Cartórios). Brasília, DF, 1994b. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L8935.htm. Acesso em: 30 mar. 2020.

BRASIL. Presidência da República. Casa Civil. *Lei nº. 10.406, de 10 de janeiro de 2002*. Institui o Código Civil. Brasília, DF, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/110406.htm. Acesso em: 30 mar. 2020.

BRASIL. Presidência da República. Casa Civil. *Lei nº. 11.977, de 7 de julho de 2009*. Dispõe sobre o Programa Minha Casa, Minha Vida – PMCMV e a regularização fundiária de assentamentos localizados em áreas urbanas... Brasília, DF, 2009. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/L11977compilado.htm. Acesso em: 30 mar. 2020.

BRASIL. Presidência da República. Casa Civil. *Lei nº. 12.682, de 09 de julho de 2012*. Dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos. Brasília, DF, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12682.htm. Acesso em: 30 mar. 2020.

BRASIL. Presidência da República. Casa Civil. *Lei nº. 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/L12965.htm. Acesso em: 30 mar. 2020.

BRASIL. Presidência da República. Casa Civil. *Lei nº. 13.105, de 16 de março de 2015*. Código de Processo Civil. Brasília, DF, 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/L13105.htm. Acesso em: 30 mar. 2020.

BRASIL. Presidência da República. Casa Civil. *Lei nº. 13.874, de 20 de setembro de 2019*. Institui a Declaração de Direitos de Liberdade Econômica; estabelece garantias de livre mercado... Brasília, DF, 2019a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13874.htm. Acesso em: 30 mar. 2020.

BRASIL. Presidência da República. Casa Civil. *Medida Provisória nº. 2.200-2, de 24 de agosto de 2001*. Institui a Infraestrutura de Chaves Públicas Brasileira – ICP – Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Brasília, DF, 2001. Disponível em: http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm. Acesso em: 30 mar. 2020.

CENTRAL RTDPJBRASIL. Disponível em: <https://www.rtdbrasil.org.br/>. Acesso em: 30 mar. 2020.

PAIVA, J. P. L. *Direito registral registros públicos*. 2009. Disponível em: http://www.lama-napaiva.com.br/banco_arquivos/registros_publicos.pdf. Acesso em: 30 mar. 2020.

PAIVA, J. P. L. Registro eletrônico. In: ENCONTRO DO COMITÊ LATINO AMERICANO DE CONSULTA REGISTRAL, 27., 2015, Cuba. *Apresentação de Trabalho* [...]. Havana: IPDR, 2015. Disponível em: <http://registrodeimoveis1zona.com.br/wp-content/uploads/2014/07/REGISTRO-ELETRONICO-Brasil.pdf>. Acesso em: 30 mar. 2020.

PINHO, R. V. P. R. *Registro em meio eletrônico*: consulta. Destinatário: Dra. Sonia Cantelmo. Osasco, SP, [2020?]. 1 e-mail. Disponível em: <http://2osasco.com.br/registroeletronico.pdf>. Acesso em: 30 mar. 2020.

RODRIGUES, M. G. *Registros públicos*: visão geral, aspectos relevantes, importância para a democracia. 2007. 1 palestra [Palestra proferida na Escola Judicial Des. Edésio Fernandes, TJMG]. Disponível em: <https://bd.tjmg.jus.br/jspui/bitstream/tjmg/702/1/palRM-REG.pdf>. Acesso em: 30 mar. 2020.

Leitura recomendada

CAMPINAS. 1º Oficial de Registro de Títulos e Documentos e Civil de Pessoa Jurídica. *Registro de documentos*. Disponível em: <http://cartoriortdcampinas.com.br/registro-de-documentos/>. Acesso em: 30 mar. 2020.



Fique atento

Os *links* para *sites* da *web* fornecidos neste capítulo foram todos testados, e seu funcionamento foi comprovado no momento da publicação do material. No entanto, a rede é extremamente dinâmica; suas páginas estão constantemente mudando de local e conteúdo. Assim, os editores declaram não ter qualquer responsabilidade sobre qualidade, precisão ou integralidade das informações referidas em tais *links*.

Sistema de registro eletrônico de títulos e documentos

Objetivos de aprendizagem

Ao final deste texto, você deve apresentar os seguintes aprendizados:

- Explicar as diretrizes gerais do sistema de registro eletrônico de títulos e documentos.
- Reconhecer as vantagens do sistema de registro eletrônico de títulos e documentos.
- Discutir a respeito da privacidade e da proteção dos dados pessoais no sistema de registro eletrônico de títulos e documentos.

Introdução

A Lei nº. 11.977, de 7 de julho de 2009 (BRASIL, 2009), instituiu o sistema de registro eletrônico e a sua obrigatoriedade em relação aos registros públicos. O registro eletrônico nos escritórios de registros em geral e no próprio registro de títulos e documentos representa um fato inevitável que se fundamenta na necessidade de compartilhamento rápido e eficiente de fatos e negócios jurídicos relevantes por meio de canais digitais e sistemas eletrônicos. Porém, a consolidação de bancos de dados amplos pode trazer riscos de ofensa aos direitos da privacidade e ocasionar uma ampla divulgação de dados pessoais, que devem ser protegidos.

Neste capítulo, você vai ler sobre as diretrizes para o sistema eletrônico dos registros de títulos e documentos, além de reconhecer as vantagens desse sistema no acesso e na transmissão de documentos registrados e registráveis. Por fim, poderá conhecer mais sobre os riscos do amplo compartilhamento de dados por meio do registro eletrônico, que podem acabar violando o direito à privacidade, o que exige atenção na proteção de dados e documentos pessoais nas serventias de registro.

1 Diretrizes gerais de registro eletrônico de títulos e documentos

A revolução digital teve seu início situado entre o final dos anos 1950 e início dos anos 1970. Trata-se de um processo em curso que segue até a atualidade. Esse processo importa na constituição de computadores digitais e constituição de arquivos digitais em detrimento da tecnologia mecânica e analógica.

A criação e a ampla utilização dos dados digitais têm e tiveram reverberações jurídicas importantes, com a criação de novas legislações regulatórias, a partir da discussão sobre a validade como meio de prova, sobre a segurança de dados, além de muitas outras. A digitalização dos dados altera também as formas de prestação de trabalho e as próprias ferramentas laborais.

Em relação à atividade jurídica, a digitalização deu origem, por exemplo, à criação — pelo Conselho Nacional de Justiça (CNJ), em parceria com diversos tribunais e outras entidades — do **Processo Judicial Eletrônico (PJe)**, que objetiva a padronização nacional da prestação judiciária eletrônica por meio de um único sistema. Um importante marco de digitalização em relação às serventias de registro é a Lei nº. 11.977/2009 (BRASIL, 2009), que instituiu o registro eletrônico, posteriormente regulamentado pelo Provimento nº. 48, de 16 de março de 2016 (BRASIL, 2016), e pelo Provimento nº. 59, de 3 de maio de 2017 (BRASIL, 2017), do CNJ.

Como afirma Loureiro (2017), a maior parte das grandes cidades brasileiras já possuía um sistema eletrônico e um banco de dados eletrônicos, que continham registros e averbações, mas o banco de dados servia exclusivamente para facilitar a prestação dos serviços. Desse modo, não possuíam valor legal, sendo ainda obrigatórias a manutenção e a conservação de livros em formato de papel.



Saiba mais

Os documentos para registro poderão ser apresentados em formato eletrônico, desde que atendam aos requisitos da Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil) e à arquitetura de Padrões de Interoperabilidade de Governo Eletrônico (e-PING), além da expedição de traslados e certidões dos registros lavrados com assinatura eletrônica. Desse modo, passa a ser possível tanto a apresentação ou expedição de documento em formato digital como a expedição de traslados e certidões em formato digital, sem a necessidade de sua apresentação em papel.

O art. 39, *caput*, da Lei nº. 11.977/2009 (BRASIL, 2009) estabelece que os atos registrais praticados a partir da vigência da Lei de Registros Públicos (Lei nº. 6.015, de 31 de dezembro de 1973) (BRASIL, 1973) deverão ser inseridos no sistema de registro eletrônico no prazo de 5 anos, contados da vigência daquela lei, que entrou em vigor na data de sua publicação. O artigo também determina que até mesmo os atos anteriores à vigência da Lei de Registros Públicos devem ser inseridos no sistema de registro eletrônico, mas não estabelece um prazo para isso (art. 39, § 1º, da Lei nº. 11.977/2009) (BRASIL, 2009).

Loureiro (2017) aponta que a lei não deixa claro se é necessário manter os livros em formato de papel e os livros eletrônicos, mas, pela lógica, esses livros não serão mais necessários, posto que o art. 40 da referida lei estabelece a obrigatoriedade de criar cópias de segurança dos documentos e livros digitalizados. Desse modo, seria ilógica a guarda também dos livros em formato de papel.

Por fim, o art. 41 da Lei nº. 11.977/2009 (BRASIL, 2009) prevê que, após a implementação dos sistemas eletrônicos, os serviços de registro público devem disponibilizar, por meio eletrônico e sem ônus, ao Poder Judiciário e Poder Executivo federal o acesso às informações constantes em seus bancos de dados.

A referida lei instituiu o sistema eletrônico de registro, contudo, esse sistema está previsto em apenas cinco artigos, ficando a regulamentação e a forma de registro a cargo do CNJ e das Corregedorias de Justiça dos Estados e do Distrito Federal.

Na regulamentação do sistema de registro eletrônico, o Provimento nº. 48/2016 (BRASIL, 2016) do CNJ traz as principais regulamentações e estabelece, em seu art. 2º, que o sistema de registro eletrônico deve ser implementado e integrado por todos os oficiais de registro. Esse sistema compreende:

Art. 2º [...]

I — o intercâmbio de documentos eletrônicos e de informações entre os órgãos de registro de títulos e documentos e civil de pessoas jurídicas, o Poder Judiciário, a Administração Pública e o público em geral;

II — a recepção e o envio de títulos em formato eletrônico;

III — a expedição de certidões e a prestação de informações em formato eletrônico;

IV — a formação, nos cartórios competentes, de repositórios registrais eletrônicos para o acolhimento de dados e o armazenamento de documentos eletrônicos;

V — a recepção de títulos em formato físico (papel) para fins de inserção no próprio sistema, objetivando enviá-los para o registro em cartório de

outra comarca (inserido pelo Provimento nº. 59 do CNJ) (BRASIL, 2016, documento *on-line*).

Assim, além da recepção e do envio de títulos em formato eletrônico, as serventias devem realizar o intercâmbio eletrônico de documentos. É possível, inclusive, o protocolo de documento em comarca diversa do registro originário, quando o ofício de registro que recebeu o documento deve encaminhá-lo eletronicamente à serventia competente para o registro.

O art. 3º do Provimento nº. 48/2016 (BRASIL, 2016) do CNJ prevê a criação de centrais de serviços eletrônicos compartilhados em cada um dos Estados e no Distrito Federal, propiciando o intercâmbio de documentos entre os diversos serviços de registro.

Hoje em dia, na prática, foi criada, em 2012, a Central Nacional de Registro de Títulos e Documentos e de Registro Civil de Pessoas Jurídicas (Central RTDPJBrasil) pelos próprios oficiais de registro do Brasil, que propicia o intercâmbio de informações entre as serventias de registro, além de permitir diversos serviços, como:

- coleta de assinaturas com certificado digital;
- registros de documentos e arquivos digitais;
- pedidos de certidão;
- solicitações de notificações extrajudiciais;
- consulta à validade de registros e certidões (CENTRAL RTDPJBRA-SIL, 2020).

A central de serviços eletrônicos partilhados é o único responsável pelo processamento e atendimento de solicitações, além de ser o único responsável pelo envio dessas solicitações ao ofício de registro competente (art. 4º do Provimento nº. 48/2016 do CNJ) (BRASIL, 2016). Contudo, isso não significa que o controle, a guarda e a conservação dos documentos e dados eletrônicos sejam relegados ao serviço de compartilhamento. A responsabilidade sobre os arquivos e dados eletrônicos é de cada um dos oficiais de registro nos quais o registro foi realizado (art. 4º, parágrafo único, do Provimento nº. 48/2016 do CNJ) (BRASIL, 2016).

O art. 6º do Provimento nº. 48/2016 (BRASIL, 2016) autoriza a utilização de sistemas de computação, microfilmagem, disco óptico ou outros meios de reprodução para a escrituração dos livros de registro, que devem ser mantidos pelas serventias. O artigo também relega às Corregedorias-Gerais de Justiça (CGJs) dos Estados e do Distrito Federal a edição de normas técnicas para

essa guarda e conservação. Essas outras formas de guarda e conservação não excluem a escrituração eletrônica em repositórios registrais destinados a esse fim.

Os repositórios registrais eletrônicos devem receber dados das serventias, que lhes servirão como base para a criação e guarda permanente dos arquivos. Assim, devem ser observadas todas as normas relacionadas do CNJ sobre a digitalização de documentos e eventuais outras normas das Corregedorias dos tribunais locais (art. 7º, *caput*, parágrafo único, do Provimento nº. 48/2016 do CNJ) (BRASIL, 2016).



Fique atento

A utilização do sistema eletrônico para recepção ou expedição de documentos eletrônicos é obrigatória, ficando vedada a sua recepção ou expedição por *e-mail*, serviços postais ou entrega em geral (art. 8º, I, do Provimento nº. 48/2016 do CNJ) (BRASIL, 2016). Outra preocupação do CNJ é a unificação de um sistema para prestação do serviço de compartilhamento de dados. Assim, é vedada a publicação de documentos eletrônicos e informações em *sites* que não sejam das centrais de serviços compartilhados, bem como é proibida a prestação de serviços eletrônicos pelas próprias serventias ou por terceiros em concorrência com as centrais de serviços eletrônicos compartilhados ou fora delas (art. 8º, II e III, do Provimento nº. 48/2016 do CNJ) (BRASIL, 2016).

O regulamento não veda a expedição ou a recepção de documentos por sistemas eletrônicos em geral, tendo em vista que isso ocorre por meio de sistemas eletrônicos dos serviços compartilhados. O que o regulamento veda é que essas transmissões ocorram por *e-mail*. Na prática, os serviços compartilhados disponibilizam sistemas eletrônicos pelos quais os usuários podem se cadastrar e, por meio deles, expedir e recepcionar documentos.

O registro eletrônico não significa a impossibilidade de registro de documento por mídia física, ou seja, o usuário pode apresentar os documentos necessários diretamente nos cartórios ou no cartório distribuidor quando for exigido. Nesses casos, os documentos registrados são digitalizados e mantidos nos arquivos digitais dos serviços de registro. Também não é obrigatório que o documento assinado digitalmente seja enviado por meio de sistema eletrônico. Caso o usuário compareça à serventia de registro, com o documento eletrônico devidamente assinado, os cartórios devem recepcioná-los (art. 9º do Provimento nº. 48/2016 do CNJ) (BRASIL, 2016).

Em resumo, a Lei nº. 11.977/2009 (BRASIL, 2009) tornou obrigatória a criação de um sistema de registro eletrônico. Desse modo, os registros de títulos e documentos podem e devem manter um banco de dados dos títulos e documentos registrados. Apesar de a lei não proibir a existência de documentos em seu formato em papel, na prática, a opção pela digitalização do documento nas serventias extrajudiciais pode trazer diversas vantagens, que incluem até mesmo o fato de ocuparem menor espaço físico.

Até mesmo os documentos registrados antes do advento da Lei nº. 11.977/2009 podem ser digitalizados e conservados apenas em formato digital, não sendo necessárias a sua manutenção e a guarda em formato de papel. Como o registro pode ser feito por meio eletrônico — ou seja, sequer é necessária a presença do usuário em cartório, que pode enviar o documento eletronicamente e com assinatura digital —, a emissão das certidões também pode se dar por meio digital ou em formato de papel.

2 Vantagens do sistema de registro eletrônico de títulos e documentos

O registro eletrônico de documentos é uma necessidade que veio acompanhada de uma situação fática. Os bancos de dados digitais já eram uma realidade mesmo antes do advento da Lei nº. 11.977/2009, por isso, já eram amplamente utilizados pelos diversos serviços de registro nacionais, mas não tinham validade legal, posto a inexistência de lei regulatória.

Sequer havia norma que facultava o armazenamento dos documentos registrados em seu formato digital. No Brasil, o documento eletrônico e a assinatura digital têm suas origens legais desde 2001, após serem disciplinados pela Medida Provisória (MP) nº. 2.200-1, de 27 de julho de 2001, reeditada pela MP 2.200-2, de 24 de agosto de 2001 (BRASIL, 2001). Por meio dessas MPs, foi instituída a ICP-Brasil, com a finalidade de “[...] garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras” (art. 1º da MP 2.200-2/2001) (BRASIL, 2001, documento *on-line*). Assim, o documento eletrônico e a sua autenticidade garantida por assinatura eletrônica são de aproximadamente 8 anos anteriores à própria possibilidade do registro eletrônico.

Ainda que haja esse hiato temporal, o registro eletrônico instituído pela Lei nº. 11.977/2009 (BRASIL, 2009) representou um grande marco nas atividades registrais, uma vez que adequou a nova realidade das tecnologias digitais às

atividades de registro. É certo que a transmissão e a guarda de dados digitais trazem diversas vantagens em relação ao armazenamento dos documentos em seu formato em papel.

A primeira grande vantagem do sistema de registro eletrônico, tanto aplicável aos registros de títulos e documentos como às demais serventias registrais, está relacionada à própria atividade do oficial de registro. O inciso I do art. 30 da Lei dos Cartórios (Lei nº. 8.935, de 18 de novembro de 1994) estabelece que, entre os deveres dos notários e registradores, está: “Art. 30 [...] I — manter em ordem os livros, papéis e documentos de sua serventia, guardando-os em locais seguros” (BRASIL, 1994, documento *on-line*).

Essa obrigação está relacionada ao dever de custódia, guarda e conservação de seus arquivos. Os notários e registradores não são proprietários dos documentos e livros sob sua guarda, mas são apenas depositários, já que os livros e documentos pertencem, de fato, ao Estado (LOUREIRO, 2017). Tanto é que, quando um oficial de registro ou um notário é substituído por outro, acaba herdando todos os documentos e livros de seu antecessor, cabendo-lhes a sua guarda e conservação.

Após a criação do registro eletrônico, a Lei nº. 11.977/2009 (BRASIL, 2009) passou também a estabelecer, em seu art. 40, que deverão ser definidos regulamentos com os requisitos mínimos quanto a cópias de segurança de documentos e livros escriturados. Com isso, cria-se, por consequência, a obrigação de os registradores conservarem cópias de segurança de documentos e livros de forma eletrônica, o que foi regulamentado pelo Provimento nº. 74, de 31 de julho de 2018 (BRASIL, 2018a), do CNJ. A primeira vantagem do registro eletrônico se refere à facilitação da conservação de documentos em formato eletrônico em detrimento de seu formato em papel.

Os livros e documentos em papel se deterioram com o tempo, já os dados digitais, ao contrário, podem ser conservados por tempo indefinido, sem qualquer tipo de deterioração. Assim, o registro eletrônico facilita a conservação dos documentos sob a guarda dos registradores.

Do mesmo modo, o registro eletrônico facilita até mesmo a guarda dos documentos e livros, isso porque, até a vigência da Lei nº. 11.977/2009, os documentos registrados deveriam ser conservados em papel nas serventias extrajudiciais. Esse tipo de conservação exigia, muitas vezes, grandes espaços físicos e a criação de amplos arquivos para a guarda dos documentos. Ao contrário, o registro eletrônico permite o armazenamento dos dados, que certamente ocupam menos espaço físico do que documentos em formato de papel. Além disso, reduz o uso de papéis tanto pelas serventias quanto pelos

interessados nos registros, tendo em vista a possibilidade de transmissão de dados exclusivamente por meios eletrônicos.

Outra vantagem do registro eletrônico se refere à rapidez na emissão de certidões. Não é só o protocolo eletrônico que é possível, mas a própria emissão de certidão eletrônica do documento pela serventia de registro também é. A busca de documento registrado e a emissão de certidão ocorrem de maneira rápida, assim como a assinatura digital, que leva poucos instantes.



Exemplo

O sistema eletrônico de registro permite algo inédito, que é a possibilidade de unificação, em um único sistema, da emissão de certidões. Hoje em dia, não é necessário que o interessado compareça pessoalmente à serventia de registro. Assim, imaginemos que uma pessoa precise de uma certidão de um cartório que se localiza em outra comarca. Assim, não será necessário que se locomova até o local de domicílio das partes do negócio para requer uma determinada certidão.

Os efeitos de um negócio jurídico somente se perfectibilizam após ser conferida ao documento a sua publicidade legal, por meio de registro público. Por isso, em muitas situações, como forma de se precaver antes da realização de um negócio jurídico, é importante que o interessado busque informações registrais nos cartórios competentes, pois, caso já haja outro negócio com o mesmo objeto em curso, não poderá alegar desconhecimento se o negócio jurídico estiver devidamente registrado.

O registro de documentos nos registros de títulos e documentos devem ocorrer na serventia de domicílio das partes para produzir efeitos perante terceiros (art. 130 da Lei nº. 6.015/1973) (BRASIL, 1973). Por isso, caso o negócio esteja ocorrendo em local diverso do domicílio de uma das partes, será necessária a solicitação de certidões em outras comarcas. Nesses casos, a possibilidade de requisição por meio de um sistema integrado facilita a requisição das informações almejadas e agiliza o envio e a entrega da certidão.

Os registros eletrônicos — além de permitirem a transmissão eletrônica da certidão solicitada e o intercâmbio rápido de informações — permitem o protocolo eletrônico de documentos. Para o envio eletrônico de documentos, a parte interessada deve enviar o documento e o requerimento de registro por via eletrônica, que devem ser assinados digitalmente. Após serem recepcio-

nados e protocolados pela serventia, os documentos devem ser integralmente registrados em sistema de registro eletrônico.

Loureiro (2017) aponta que a grande vantagem desse sistema é que as entidades detentoras de grandes quantidades de arquivos em papel podem economizar tempo e espaço por meio do registro para fins de conservação nos registros de títulos e documentos. Essa conservação ocorre no formato digital. Assim, caso necessite do documento registrado, pode facilmente solicitar uma certidão em formato eletrônico ou em papel, que terá o mesmo valor que o original. Permite, desse modo, a digitalização do documento e o registro nos registros de títulos e documentos, não havendo mais a necessidade de manter os seus arquivos em papel.

A digitalização e a criação de um sistema eletrônico permitiram a criação de uma base de dados comum a todos os serviços de registro. Uma base de dados comum somente foi viabilizada com a criação tanto de um sistema eletrônico de registro, que reúne todas as informações sobre os documentos registrados, como da possibilidade de emissão de documento com assinatura eletrônica com a mesma validade de documentos emitidos pelos serviços de registro em formato de papel.

Mesmo antes da regulamentação, em 2016, do registro eletrônico pelos registros de títulos e documentos pelo CNJ, foi criada, em 12 de novembro de 2012, a Central RTDPJBrasil, que, na prática, reúne todos os registros de títulos e documentos e registro civil de pessoas jurídicas do Brasil. Essa entidade foi criada já com fins de viabilizar o que dispõe os arts. 37 e 38 da Lei nº. 11.977/2009 (CENTRAL RTDPJBRASIL, 2020). Em seu *site*, são oferecidos diversos serviços prestados pelas serventias de registro, de modo que é possível a requisição de certidões de qualquer ofício registrador nacional.

Essa central de registradores acompanha todo o processo de solicitação, por parte dos interessados, de documentos dos registros de títulos e documentos até sua efetiva emissão por parte do cartório competente. Trata-se de uma plataforma digital vinculada ao IRTDPJBrasil. As atividades dessa central são reguladas pelo CNJ.

O Poder Judiciário e o Poder Executivo federal também se beneficiaram com a criação dos sistemas de registros eletrônicos, uma vez que o art. 41 da Lei nº. 11.977/2009 (BRASIL, 2009) prevê o compartilhamento do banco de dados registradores com esses poderes sem ônus, ou seja, sem custos.

Loureiro (2017) aponta que esse dispositivo tem a constitucionalidade duvidosa por alguns motivos. As atividades dos registradores são exercidas em caráter privado, não podendo ser obrigados a prestar um serviço sem remuneração, exceto para os casos de registros essenciais para o exercício da

cidadania ou por casos de previsão de isenção total ou parcial previstos em lei estadual, tendo em vista que os emolumentos têm natureza de tributos, cuja competência tributária é estadual.

Loureiro (2017) observa ainda que o acesso indiscriminado do Estado às informações contidas em bancos de dados pode violar o direito à privacidade, já que muitos dados possuem natureza personalíssima, de interesse meramente individual. Desse modo, o registro eletrônico surge como uma necessidade e decorre de um processo já em curso, que permite a validade jurídica de documentos eletrônicos, bem como representa um importante avanço na agilidade e facilidade no acesso aos serviços de registro.

O registro eletrônico permite um serviço mais eficiente e rápido, uma vez que a base de dados de registros é facilmente acessível pelo cliente/interessado que busca as atividades registrais. O registro eletrônico faz parte de um processo maior de segurança jurídica e é garantia da validade de documentos eletrônicos que fazem parte da própria atuação do Poder Judiciário em suas diversas esferas.

3 Privacidade e proteção de dados pessoais no sistema de registro eletrônico de títulos e documentos

Os registros públicos, em geral, têm a função de dar publicidade à informação ou ao documento registrado, visando à oponibilidade e aos seus efeitos perante terceiros. A publicidade registral possibilita a qualquer interessado o acesso às informações registradas, sem a necessidade de apresentação da justificativa. Porém, as informações registradas não são efetivamente disponibilizadas a qualquer pessoa em todas as situações.



Fique atento

Em geral, o sigilo de informações registradas está relacionado a direitos personalíssimos, ligados à privacidade e à intimidade. Por exemplo, o registro civil de pessoas naturais não pode expedir certidão de nascimento de inteiro teor de pessoa adotada ou de pessoa que solicitou a alteração do assento de nome e sexo para adequação à identidade de gênero, salvo por requerimento próprio ou por ordem judicial.

As tecnologias de comunicação e o fluxo de dados pela internet têm impactos relevantes em relação aos direitos à privacidade, o que também se torna uma preocupação com a digitalização dos registros públicos. A primeira preocupação é de ordem prática com a digitalização de documentos e a disponibilização em bancos de dados comuns. A possibilidade de um ataque cibernético pode levar ao roubo e uso de dados para fins criminosos.

No caso das serventias extrajudiciais, parece adequada a interpretação de que, na obrigação de guarda dos documentos levados a registro, inclui-se a segurança dos bancos de dados contra os ataques cibernéticos, o que deve ser assegurado pelo titular da serventia e/ou pelas centrais de registros de sistemas eletrônicos no que lhes couber. O fato de os dados registrados serem, em regra, públicos não significa que possam ou devam ser amplamente divulgados por meios criminosos. Assim, em geral, os documentos registrados possuem publicidade, por isso, são passíveis de amplo conhecimento por qualquer interessado. O mesmo pode ser dito dos documentos registrados nos registros de títulos e documentos. A principal finalidade do registro é alcançar os efeitos práticos da publicidade registral, principalmente aqueles relacionados aos efeitos perante terceiros.

Para haver efeitos perante terceiros de um determinado documento registrado, deve haver a efetiva possibilidade de conhecimento por terceiros do documento registrado. Por isso, em regra, os documentos registrados devem ser passíveis de conhecimento integral de qualquer interessado, tendo em vista que o registro tem esta finalidade e este requisito: para haver efeitos públicos, o documento deve ser passível de conhecimento.

A principal questão relacionada aos registros de títulos e documentos e à proteção de dados pessoais e privados está ligada aos registros facultativos para fins de conservação (art. 127, VII, e art. 130 da Lei nº. 6.015/1973) (BRASIL, 1973). Não há, de fato, um consenso sobre a aplicabilidade do princípio da publicidade registral aos documentos levados a registro apenas para fins de conservação.

A Primeira Turma do Superior Tribunal de Justiça, por exemplo, no Recurso Especial nº. 858031/MG, 2006/0120381-6, de relatoria do Ministro Luiz Fux (publicado no Diário da Justiça Eletrônico em 17 de dezembro de 2008) entendeu, na análise de um caso concreto, que o registro nos registros de títulos e documentos — mesmo que para fins de conservação —, realizado de forma subsidiária ao registro competente, opera os efeitos perante terceiros, visto que o registro objetiva dar publicidade ao ato (BRASIL, 2008). Contudo, a partir de um passado mais recente, a jurisprudência e a doutrina têm apontado no sentido inverso: de que o registro apenas para fins de conservação não gera

efeitos perante terceiros, por isso, não se aplica o princípio da territorialidade ao registro para fins de conservação, uma vez que não se espera que operem os efeitos da publicidade registral.

Nesse sentido, o Provimento CGJ nº. 16/2019, que deu nova redação a dispositivo das Normas de Serviço da CGJ do Tribunal de São Paulo (SÃO PAULO, 1989), passou a considerar que não se aplica o princípio da territorialidade para os registros facultativos para fins de guarda e conservação. Além disso, esse regulamento passou a estabelecer expressamente que o registro para fins de conservação não gera efeitos perante terceiros (SÃO PAULO, 1989). Desse modo, a proteção de dados contidos nos documentos registrados nos registros de títulos e documentos, em regra, não ocorre, mesmo em sistemas de registros públicos, uma vez que a principal função dos registros é dar publicidade e garantir que o negócio jurídico entabulado afete a esfera jurídica de terceiros.

Porém, o mesmo não pode ser dito do documento para fins de conservação, no qual a publicidade formal, isto é, a possibilidade de acesso por qualquer pessoa, não é obrigatória por inexistir publicidade material (LOUREIRO, 2017). “Pelo contrário, a publicidade poderia prejudicar direito ou interesse pessoal, como o direito à privacidade, também protegido pela Constituição; ou ainda tornar conhecido um meio de prova que a parte pretenda conservar como segredo” (LOUREIRO, 2017, p. 477).

Nesses casos, como a publicidade não é obrigatória, mas é regra, o apresentante deve realizar pedido expresso para que se faça constar a proibição de certidões, a não ser a seu próprio pedido ou por ordem judicial. Por esse motivo, em relação aos registros para fins de conservação, é possível solicitar a restrição à publicidade registral e indicar quem poderá obter certidões do registro. O requerimento deve ser expresso, tendo em vista que, em regra, irá existir a publicidade registral, mesmo de documento levado a registro para fins de mera conservação.

O registro eletrônico de documentos reaviva a discussão sobre a restrição da publicidade de documento apresentado para meros fins de conservação. Nesses casos, os documentos podem conter informações personalíssimas que, caso divulgadas, poderiam ofender o princípio da privacidade. Em razão disso, segundo a melhor interpretação dos dispositivos legais, “[...] o registro para fins de conservação é facultativo, de forma que deve prevalecer o interesse individual do titular do documento, até porque as tecnologias de informação não conhecem fronteiras territoriais” (LOUREIRO, 2017, p. 495).

Obviamente, mesmo antes da existência do registro eletrônico, o registro para fins de conservação já poderia ferir os direitos à privacidade com a divulgação de dados pessoais personalíssimos. Porém, é certo que o sistema

eletrônico de registro dá virtualmente muito mais publicidade aos documentos registrados, pois, agora, as certidões de qualquer ofício de registro do País podem facilmente ser requeridas por meio da central de serviço eletrônico compartilhado. Em outros casos, os registros eletrônicos expandem, em muito, a possibilidade de acesso a dados que podem virtualmente ofender os direitos de privacidade, expondo situações e fatos personalíssimos.



Saiba mais

A Lei Geral de Proteção de Dados (LGPD) — Lei nº.13.709, de 14 de agosto de 2018 (BRASIL, 2018b) — deve entrar em vigência em 2021, após novo adiamento em razão da pandemia global de Covid-19 ao longo de 2020.

Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (art. 1º) (BRASIL, 2018b, documento *on-line*).

Trata-se de uma lei amplamente discutida durante 8 anos até a sua aprovação, que tem por objetivo regulamentar os dados pessoais da pessoa natural e da pessoa jurídica. Frente à expansão dos cadastros e do compartilhamento de dados pessoais entre empresas e outros entes governamentais ou privados, foi editada a LGPD. Tal legislação impactará as atividades registrais, pois certamente será necessário encontrar um fino equilíbrio entre a proteção de dados pessoais e a publicidade registral.

A conservação do documento e a publicidade registral são dois institutos distintos, apesar de os registros de títulos e documentos possuírem a competência para a realização de ambos. O registro para a conservação destina-se à reprodução ou transcrição do documento original em sua integralidade apenas para fins de conservação.

O registro para a conservação destina-se à proteção do documento original de eventual perda ou deterioração, tendo em vista que a certidão do documento possui os mesmos efeitos probatórios do conteúdo e da data de sua formação do que o documento original. Por outro lado, a publicidade registral objetiva a segurança jurídica de um ato ou negócio, permitindo que os efeitos de um contrato irradiem perante terceiros ao dar a todos a possibilidade de conhecer a existência dos contratos e de direitos ali transcritos (LOUREIRO, 2017).

A diferenciação entre ambos institutos é importante para se reconhecer os objetivos de cada um, bem como considerá-los frente ao fato de o registro eletrônico ser capaz de permitir a ampla transmissão de informações por todo o território nacional. Desse modo, se o registro, para fins de conservação, objetiva a mera proteção do documento, deve poder ter a sua publicidade registral limitada, uma vez que se tratam de informações que não interessam a terceiros e não se espera que produzam, naquele momento, pelo apresentante, qualquer tipo de efeitos perante terceiros.

Por outro lado, é interessante que o registro que objetiva a segurança jurídica do negócio, obtida por meio da publicidade registral, realmente integre o sistema eletrônico de registros. A globalização permitiu uma diminuição de fronteiras, por isso, os negócios são realizados, muitas vezes, entre pessoas (físicas ou jurídicas) de localidades distintas, às vezes, muito distantes. Assim, nesses casos, é importante a garantia do amplo acesso a documentos que possam ter reflexos nos negócios jurídicos realizados, o que, de fato, garante maior segurança jurídica à sociedade.

A proteção de dados pessoais e informações privadas no sistema de registro eletrônico passa por dois fatos: o primeiro refere-se à proteção em si do sistema contra os ataques cibernéticos ou compartilhamento indevido de informações, inclusive porque os registradores têm o dever de sigilo sobre a documentação e os assuntos de natureza reservada (art. 30, VI, da Lei nº. 8.935/1994) (BRASIL, 1994). O segundo aspecto está relacionado à possibilidade de ser solicitado o sigilo das informações registradas apenas para fins de conservação, tendo em vista que muitos documentos possuem informações pessoais e personalíssimas, devendo prevalecer, nesses casos, o interesse do particular titular do documento registrado.

A discussão sobre a proteção de dados pessoais é bastante ampla e decorre do fácil e rápido compartilhamento de dados entre instituições. Deve considerar ainda os diversos *software* e algoritmos capazes de cruzar informações para consolidar perfis pessoais de todos os membros da sociedade. Tais coletâneas de dados acabam sendo reunidas nos *big data* e em bases de dados de diversas pessoas, podendo ser utilizados para diversas finalidades, como:

- propaganda direcionada;
- manipulação de informações;
- comportamentos a partir de determinados perfis.

O *big data* fornece material para verdadeiros psicogramas da população, construindo psicogramas individuais e coletivos de toda a população (HAN,

2015). Essa situação torna premente a discussão sobre o compartilhamento de dados e a publicidade registral, uma vez que o Estado, por meio de seus sistemas de registros públicos, pode acabar fornecendo diversos dados capazes de violar direitos pessoais e da personalidade.



Referências

BRASIL. Conselho Nacional de Justiça. Corregedoria Nacional de Justiça. *Provimento n. 48, de 16 de março de 2016*. Estabelece diretrizes gerais para o sistema de registro eletrônico de títulos e documentos e civil de pessoas jurídicas. Brasília, DF, 2016. Disponível em: https://atos.cnj.jus.br/files//provimento/provimento_48_16032016_16032018112202.pdf. Acesso em: 21 maio 2020.

BRASIL. Conselho Nacional de Justiça. Corregedoria Nacional de Justiça. *Provimento n. 59, de 03 de maio de 2017*. Altera o Provimento CN-CNJ n. 48, de 16 de março de 2016, que estabelece diretrizes gerais para o sistema de registro eletrônico de títulos e documentos e civil de pessoas jurídicas. Brasília, DF, 2017. Disponível em: https://atos.cnj.jus.br/files//provimento/provimento_59_03052017_19032018114604.pdf. Acesso em: 21 maio 2020.

BRASIL. Conselho Nacional de Justiça. Corregedoria Nacional de Justiça. *Provimento n. 74, de 31 de julho de 2018*. Dispõe sobre padrões mínimos de tecnologia da informação para a segurança, integridade e disponibilidade de dados para a continuidade da atividade pelos serviços notariais e de registro do Brasil e dá outras providências. Brasília, DF, 2018a. Disponível em: https://atos.cnj.jus.br/files//provimento/provimento_74_31072018_01082018113730.pdf. Acesso em: 21 maio 2020.

BRASIL. Presidência da República. Casa Civil. *Lei n. 6.015, de 31 de dezembro de 1973*. Dispõe sobre os registros públicos e dá outras providências. Brasília, DF, 1973. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L6015compilada.htm. Acesso em: 21 maio 2020.

BRASIL. Presidência da República. Casa Civil. *Lei n. 8.935, de 18 de novembro de 1994*. Regulamenta o art. 236 da Constituição Federal, dispondo sobre serviços notariais e de registro (Lei dos Cartórios). Brasília, DF, 1994. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L8935.htm. Acesso em: 21 maio 2020.

BRASIL. Presidência da República. Casa Civil. *Lei n. 11.977, de 7 de julho de 2009*. Dispõe sobre o Programa Minha Casa, Minha Vida — PMCMV e a regularização fundiária de assentamentos localizados em áreas urbanas... Brasília, DF, 2009. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/L11977compilado.htm. Acesso em: 21 maio 2020.

BRASIL. Presidência da República. Casa Civil. *Lei n. 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 21 maio 2020.

BRASIL. Presidência da República. Casa Civil. *Medida Provisória n. 2.200-2, de 24 de agosto de 2001*. Institui a Infraestrutura de Chaves Públicas Brasileira — ICP — Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Brasília, DF, 2001. Disponível em: http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm. Acesso em: 21 maio 2020.

BRASIL. Superior Tribunal de Justiça. Recurso Especial: REsp 858.031 — MG (2006/0120381-6). Recorrente: Estado de Minas Gerais. Recorrido: Jacy Cláudio Maciel — Espólio. Relator: Ministro Luiz Fux. Brasília, DF, 2008. *Diário de Justiça*, 17 dez. 2008. Disponível em: <https://stj.jusbrasil.com.br/jurisprudencia/2351992/recurso-especial-resp-858031-mg-2006-0120381-6/inteiro-teor-12222787?ref=juris-tabs>. Acesso em: 21 maio 2020.

CENTRAL RTDPJBRASIL. Disponível em: <https://www.rtdbrasil.org.br/>. Acesso em: 21 maio 2020.

HAN, B.-C. *Psicopolítica*. Lisboa: Relógio D'Água, 2015.

LOUREIRO, L. G. *Registros públicos: teoria e prática*. 8. ed. Salvador: Juspodivm, 2017.

SÃO PAULO. Tribunal de Justiça. Corregedoria Geral da Justiça do Estado. *Provimento n. 58/89 — Normas de Serviço: Cartórios Extrajudiciais — Tomo II*. São Paulo, 1989. Disponível em: http://www.tjsp.jus.br/Download/Corregedoria/NormasExtrajudiciais/NSCGJ_TOMO_II_NORMAL.pdf. Acesso em: 21 maio 2020.



Fique atento

Os *links* para *sites* da *web* fornecidos neste capítulo foram todos testados, e seu funcionamento foi comprovado no momento da publicação do material. No entanto, a rede é extremamente dinâmica; suas páginas estão constantemente mudando de local e conteúdo. Assim, os editores declaram não ter qualquer responsabilidade sobre qualidade, precisão ou integralidade das informações referidas em tais *links*.

Contratos eletrônicos

Camila Coelho Moreira

OBJETIVOS DE APRENDIZAGEM

- > Reconhecer a importância da proteção dos consumidores frente aos contratos eletrônicos.
- > Explicar o que é assinatura digital.
- > Analisar a jurisprudência das cortes superiores acerca dos contratos eletrônicos.

Introdução

A chegada da internet com suas facilidades no Brasil e no mundo foi um marco muito importante para a nossa sociedade, pois revolucionou as formas de agir, de pensar, de se relacionar e de celebrar negócios jurídicos, que passaram a se adequar ao meio eletrônico, facilitando as relações a distância. Com isso, surgiu a necessidade de regulamentação dessas novas formas de contratação, considerando suas peculiaridades, bem como a necessidade de resguardar as pessoas envolvidas na relação jurídica contra qualquer tipo de abuso ou irregularidade, com base no que se encontra disposto na legislação civil brasileira vigente e na Constituição Federal.

Neste capítulo, você vai estudar a importância e o histórico da proteção dos consumidores no mercado de consumo, a legitimidade das assinaturas digitais, muito utilizadas nessas modalidades de contratação, além das decisões judiciais sobre o tema.

Proteção dos consumidores

O direito do consumidor é um tema relativamente novo no ordenamento jurídico brasileiro, se considerarmos que o Código de Proteção e Defesa do Consumidor (CDC) surgiu somente em 1990 e que somente após a promulgação da Constituição de 1988 foi elevado ao *status* de direito indisponível. Antes dessa data, não havia no Brasil qualquer tipo de regulamentação específica ou proteção consolidada voltada para essa categoria de indivíduos, que dentro da relação consumerista eram tratados em tom de paridade com a outra parte, o fornecedor (CAVALIERI FILHO, 2019).

A proteção do consumidor como grupo vulnerável consiste em uma necessidade que surgiu há muito tempo na história, a partir da ascensão do capitalismo, responsável pelo crescimento das relações de consumo no mundo. Registros históricos datados do século XVIII a.C. já apontavam a existência de regulamentos esparsos que buscavam, de certa forma, proteger a figura do consumidor contra qualquer tipo de vantagem excessiva. Um exemplo é a regulamentação quanto ao estabelecimento de preços e direitos e obrigações dos profissionais liberais presentes no Código de Hamurabi. Ainda na Idade Média, na França, eram previstos castigos físicos aos falsificadores, na tentativa de impedir tal prática desleal (CAVALIERI FILHO, 2019). Tais informações já demonstravam a necessidade de intervenção do Estado na proteção dessa categoria de sujeitos.

O crescimento do mercado de consumo marcado pela Revolução Industrial, responsável por criar um novo modelo de sociedade, fez com que as pessoas migrassem dos campos para a cidade e, a partir do surgimento das indústrias, houve um grande apelo por produtos e serviços. Os fornecedores, além de fabricarem um produto ou prestarem um serviço, passaram a ter que se preocupar com a demanda da época e, com isso, deixaram de lado o aspecto qualitativo, focando no aspecto quantitativo, na produção em massa.

Essa mudança do mercado passou a influenciar diretamente na relação jurídica estabelecida entre as partes, uma vez que a relação contratual bilateral estabelecida entre fornecedor e consumidor, desde a contratação até a entrega do produto e/ou serviço, foi substituída por uma relação unilateral, em que o fornecedor passou a ditar as regras de contratação e composição do produto, cabendo ao consumidor aceitá-la ou não. Se você quisesse adquirir uma determinada roupa, você precisava ir até o fabricante de tecido, escolher a qualidade do pano e levá-lo até a costureira, que, juntamente a você, pactuaria de que forma aquela peça de roupa seria feita, os aviamentos e adornos utilizados, o tamanho da peça, o prazo de entrega do produto e o valor do serviço. Hoje,

as lojas contratam uma gama de costureiras, selecionam o tecido conforme sua conveniência e produzem as peças de roupa conforme a demanda e os pedidos que ela recebe. A você, consumidor final, não cabe mais participar do processo de escolha da matéria-prima, da elaboração da peça ou, até mesmo, de combinar uma forma de pagamento específica entre vocês, pois agora a sua opção é adquirir ou não o produto e aderir ou não às condições do fornecedor. Note que a participação do consumidor nas etapas do contrato e da fabricação do produto foi cada vez mais sendo deixada de lado, pois não se tinha mais tempo para negociação, tendo em vista a alta demanda que o mercado exigia. Com isso, os contratos de adesão foram dominando as relações consumeristas, e a relação jurídica, que antes era bilateral, transformou-se em uma relação jurídica unilateral, em que somente uma parte dita as regras e detém o domínio das matérias-primas para a produção do bem de consumo.

Essa ausência de participação do consumidor dá origem a sua vulnerabilidade, pois agora não cabe ao ele qualquer tipo de protagonismo ou participação dentro da relação consumerista, sendo tal protagonismo concentrado nas mãos do fornecedor. Considera-se que a vulnerabilidade do consumidor está relacionada com dois principais atos: o de somente aderir aos contratos de consumo e não mais participar de sua elaboração, bem como o de adquirir o produto sem conhecer suas especificidades técnicas ou a qualidade de sua matéria-prima (CAVALIERI FILHO, 2019).

A partir dessa nova mudança de paradigma, era inevitável que problemas comesçassem a surgir. Com a ausência de participação do consumidor durante a produção e com o consequente aumento da demanda do mercado e da valorização da quantidade em detrimento à qualidade, a produção em massa e a busca exacerbada pelo domínio de mercado, assim como o lucro, fizeram com que diversas empresas passassem a atuar de forma desleal e desonesta. Por conta da ausência de conhecimento ou, até mesmo, de certa vulnerabilidade, os consumidores tornaram-se vítimas de tal prática predatória. Adaptaram-se a produtos ou serviços que não têm a qualidade de outrora e que passaram a apresentar os chamados vícios, defeitos capazes de causar ao consumidor diversos prejuízos, sejam eles de origem econômica ou física.

Diante dessas questões, ao questionar juridicamente acerca dos atos lesivos encarados, o consumidor não tinha proteção alguma. Isso porque, na relação comercial entre fornecedor e consumidor, a legislação existente tratava as partes do contrato de maneira equivalente, assim como os demais contratos sujeitos à legislação civil, desconsiderando o desequilíbrio derivado de tal relação, bem como a vulnerabilidade da figura do consumidor. O direito do consumidor surge, portanto, como uma forma de interferência do Estado

na relação privada para reequilibrar a relação contratual com um tratamento desigual com base nas desigualdades entre as partes, com o fim de tornar as relações contratuais minimamente justas.



Saiba mais

Um discurso realizado pelo presidente dos Estados Unidos em 1962, John F. Kennedy, foi considerado um dos mais importantes na história dos direitos do consumidor, pois, além de enumerar os direitos, propôs uma reflexão jurídica sobre o tema, considerando-o um novo desafio para todo o mercado. Na fala do presidente, ele lembrou que todos somos consumidores em algum momento de nossas vidas, ou seja, que inevitavelmente em alguma parte de nossas vidas teremos esse papel na sociedade e na economia, de modo que tais direitos ou interesses, ao mesmo tempo em que são individuais, também são coletivos, em prol de um grupo que pode ser identificado ou não. Logo em seguida, no ano de 1985, a Organização das Nações Unidas estabeleceu diretrizes para a criação de um direito específico voltado para o consumidor e reforçou a ideia de que se trata de uma categoria de direito humano de nova geração (ou dimensão):

[...] um direito social e econômico, um direito de igualdade material do mais fraco, do leigo, do cidadão civil nas suas relações privadas frente aos profissionais, os empresários, as empresas, os fornecedores de produtos e serviços, que nesta posição são experts, parceiros considerados “fortes” ou em posição de poder (BENJAMIN; MARQUES; BESSA, 2010, p. 28).

O CDC reconhece, em seu art. 4º, a vulnerabilidade do consumidor e, ao longo do dispositivo legislativo, divide-a em três categorias principais: técnica, econômica e jurídica. A **vulnerabilidade técnica** existe porque o fornecedor detém toda a informação a respeito do produto ou serviço colocado no mercado, bem como é o fornecedor que impõe as condições de comercialização de determinado produto e/ou serviço. A **vulnerabilidade econômica** está relacionada com o fato de que o fornecedor é quase sempre economicamente mais poderoso que o consumidor, fato que por si só o coloca em vantagem. A terceira é a **vulnerabilidade jurídica** e deriva da econômica, pois está relacionada com o fato de que os fornecedores, em grande parte, têm mais informações jurídicas e contam com um corpo jurídico mais qualificado do que os consumidores, que sequer têm ciência de seus direitos (BRASIL, 1990). Há ainda uma quarta categoria de vulnerabilidades, que é considerada como uma evolução das demais, a denominada **vulnerabilidade de informação**, que surge na era digital e está relacionada ao controle das informações transmitidas pelos fornecedores.

Destaca-se, ainda, no viés protecionista e da evolução dos direitos do consumidor, o Marco Civil da Internet, com a entrada em vigor da Lei nº. 12.965,

de 23 de abril de 2014, importante na proteção dos consumidores no meio digital. No que tange à realização de contratos em meio eletrônico, o Marco Civil dispõe, em seu art. 7º, inciso VIII, que “[...] os contratos de prestação de serviços entre provedores e usuários deverão conter informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de dados pessoais” (BRASIL, 2014, documento *on-line*). Já em seu art. 8º, parágrafo único, incisos I e II, do mesmo diploma, dispõe que as cláusulas contratuais:

[...] serão nulas de pleno direito quando implicarem em violação ao sigilo das comunicações privadas, pela internet, ou, quando em contrato de adesão, não oferecerem como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no território nacional (BRASIL, 2014, documento *on-line*).

Não há como negar que a revolução causada pela informatização do mundo moderno pela internet foi considerada um grande marco no direito do consumidor, tendo em vista o aumento exponencial das relações de consumo por meios eletrônicos. Isso foi potencializado ainda mais durante a pandemia de covid-19, responsável por um aumento exponencial nas compras *on-line*, o que por via de consequência demandou mais esforços para a proteção e defesa dos consumidores. Os requisitos jurídicos para a validade das negociações precisaram se adequar às novas tecnologias, e a proteção dessa categoria de indivíduos precisou ser redobrada.

Assinatura digital

Você já se deu conta de quantos contratos celebra por dia, por semana, por mês? Essa pode parecer uma pergunta um pouco diferente, mas hoje vivemos em um mundo tão acelerado e tão moderno que, em um dia, por vezes, celebramos diversos negócios jurídicos sem perceber. Foi-se a época em que celebrar um contrato era sinônimo de assinar folhas e folhas de papel. Essa foi uma das facilidades que surgiram com a internet, que transformou de maneira significativa a forma com que as pessoas contratam serviços e compram produtos.

Durante o ato de celebração de um negócio jurídico, o consentimento das partes se traduz como um dos requisitos obrigatórios, conforme está disposto no Código Civil (BRASIL, 2002). Tal consentimento consiste na manifestação de vontade das partes, na concordância com os termos e cláusulas dispostas, que irão regulamentar a relação jurídica ali estabelecida. Com a modernização do mercado e da própria sociedade, essa anuência aos termos de um acordo

ou contrato por meio da assinatura de papéis se transformou e deu lugar à assinatura digital.

Imagine que você tem uma grande empresa e quer comprar insumos da China, pois tal negociação seria capaz de diminuir significativamente os custos da sua produção, aumentando seu lucro. Em sites de busca, você consegue o contato do CEO da empresa chinesa e marca uma reunião. No dia e na hora combinados, daqui do Brasil, faz uma videochamada com o empresário chinês. Vocês, então, chegam a um acordo que seria vantajoso para ambas as partes, mas a formalização em ambos os países, por questões burocráticas, exige a assinatura e o reconhecimento de firma das partes. Perceba que tal procedimento levaria dias, semanas ou até meses, se considerarmos a distância entre os dois países, o que tornaria todo o processo moroso, custoso e incompatível com a nova realidade experimentada por todos no mundo.

A partir dessa necessidade, surgiram as assinaturas eletrônicas, modalidade que revolucionou os negócios jurídicos no mundo moderno e facilitou a vida das pessoas e das empresas, pois, além de consistir em uma forma remota de manifestação da vontade, também é uma forma de verificação da autenticidade, reduzindo custos e atribuindo uma maior segurança aos negócios. A assinatura digital é aquela relacionada a qualquer processo eletrônico que indica a aceitação de um contrato ou registro, por meio de uma autenticação eletrônica, como *e-mail*, usuário corporativo ou, até mesmo, um PIN específico fornecido por uma empresa.

A assinatura digital é uma espécie de assinatura eletrônica, uma tecnologia que utiliza métodos matemáticos (criptografia) para vincular o documento eletrônico a ser assinado com o certificado digital do assinante. No Brasil, surge em 2001, com a entrada em vigor da Medida Provisória nº. 2.200, de 28 de junho de 2001, que instituiu a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), cujo objetivo é garantir autenticidade, integridade e validade jurídica de documentos de forma eletrônica, tanto das aplicações de suporte, quanto das aplicações habilitadas que utilizem certificados digitais, com o fim de assegurar a realização de transações eletrônicas seguras (BRASIL, 2001a). Consiste em um conjunto de entidades, padrões técnicos e regulamentos criados para dar suporte a um sistema criptográfico com base nos certificados digitais, os quais serão demonstrados detalhadamente a seguir.

Organização do ICP-Brasil

O ICP-Brasil consiste em um conjunto de entidades, políticas, normas, regulamentos, sistemas, mecanismos criptográficos e técnicas de gestão, cuja

finalidade é tornar a criptografia de chaves públicas acessível, viabilizando a sua utilização sem deixar de garantir a autenticidade exigida. Atualmente, a ICP-Brasil é composta pelo Comitê Gestor, Comitê Técnico, Autoridade Certificadora Raiz, Autoridades Certificadoras (AC) e Autoridades de Registro (AR).

O Comitê Gestor, na estrutura organizacional do ICP-Brasil, é o responsável pela coordenação, implantação e funcionamento de todo o sistema. Segundo disposto no art. 4º da MP nº. 2.200-2/2001, compete ao Comitê Gestor:

- I – adotar as medidas necessárias e coordenar a implantação e o funcionamento da ICP-Brasil;
- II – estabelecer a política, os critérios e as normas técnicas para o credenciamento das AC, das AR e dos demais prestadores de serviço de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação;
- III – estabelecer a política de certificação e as regras operacionais da AC Raiz;
- IV – homologar, auditar e fiscalizar a AC Raiz e os seus prestadores de serviço;
- V – estabelecer diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionais das AC e das AR e definir níveis da cadeia de certificação;
- VI – aprovar políticas de certificados, práticas de certificação e regras operacionais, credenciar e autorizar o funcionamento das AC e das AR, bem como autorizar a AC Raiz a emitir o correspondente certificado;
- VII – identificar e avaliar as políticas de ICP externas, negociar e aprovar acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional, certificar, quando for o caso, sua compatibilidade com a ICP-Brasil, observado o disposto em tratados, acordos ou atos internacionais; e
- VIII – atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança (BRASIL, 2001b, documento *on-line*).

O Comitê Técnico tem o papel de auxiliar e, como o próprio nome sugere, atua fornecendo suporte técnico ao Comitê Gestor na tomada de decisões. A Autoridade Certificadora Raiz (AC-Raiz) é a primeira autoridade certificadora da cadeia e é responsável por executar as políticas de certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor. Segundo o art. 5º da lei, suas funções consistem em:

[...] emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subsequente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de fiscalização e auditoria das AC e das AR e dos prestadores de serviço habilitados na ICP, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil, e exercer outras atribuições que lhe forem cometidas pela autoridade gestora de política (BRASIL, 2001b, documento *on-line*).

Seguindo a estrutura organizacional, temos as Autoridades Certificadoras, hierarquicamente inferiores à AC-Raiz, credenciadas e aptas a emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular. Às ACs compete “[...] emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações” (BRASIL, 2001b, documento *on-line*). Abaixo das ACs estão as ARS, que consistem em entidades operacionalmente vinculadas à determinada AC. Compete-lhes “[...] identificar e cadastrar usuários, encaminhar solicitações de certificados às AC e manter registros de suas operações” (BRASIL, 2001b, documento *on-line*). Por fim, dentro dessa cadeia, existem os Titulares dos Certificados, consideradas as pessoas físicas ou jurídicas que podem ser titulares dos certificados digitais emitidos por uma das ACS integrantes da ICP-Brasil.

De acordo com o art. 10 da MP 2.200-2/2001, os documentos eletrônicos assinados digitalmente com o uso de certificados emitidos no âmbito da ICP-Brasil têm a mesma validade jurídica que os documentos escritos com assinaturas manuscritas (BRASIL, 2001b). No entanto, é possível que as partes escolham outro meio de comprovação de autoria e integridade dos documentos de forma eletrônica, inclusive não emitidos pela ICP-Brasil, desde que tal pactuação seja prévia e aceita pela pessoa a quem for oposto o documento (BRANCHER, 2018).



Saiba mais

A mera existência da assinatura digital não é capaz de tornar um contrato válido, pois é apenas um requisito essencial quanto à formalidade do contrato eletrônico, a anuência. O contrato eletrônico, assim como os demais contratos regulamentados pelo Código Civil Brasileiro precisam atender a outros requisitos, como capacidade das partes, a licitude do objeto e a forma, que deve ser prescrita ou não defesa em lei (BRASIL, 2002).

Portanto, a assinatura digital é de grande valia na verificação da presunção de sua veracidade, uma forma de autenticação daquele usuário, trazendo maior autenticidade e segurança para o negócio jurídico. Vale ressaltar que outros elementos e requisitos de validade estão relacionados com o contrato eletrônico. Além disso, a prática jurídica diária e as relações contratuais estabelecidas no dia a dia fazem com que o direito se adeque a essa nova realidade, sendo, inclusive, assunto repercutido nos tribunais superiores.

Contratos eletrônicos: entendimento das cortes superiores

A realização de contratações pela internet se tornou indispensável na vida moderna. Tal avanço tecnológico capaz de promover alterações na sociedade fez com que, inevitavelmente, conflitos oriundos dessas contratações surgissem, resultando em ações judiciais que versam sobre o tema nos tribunais superiores.

Antes de comentarmos algumas decisões importantes, precisamos fazer algumas considerações iniciais sobre os contratos eletrônicos. Atualmente no Brasil, a forma eletrônica é entendida somente como um meio específico de realização da contratação, de modo que os demais requisitos contratuais obrigatórios estipulados pelo Código Civil devem ser mantidos. Vejamos:

DIREITO DO CONSUMIDOR. AÇÃO DE COBRANÇA. CONTRATO ELETRÔNICO. ALEGADA AUSÊNCIA DOS TERMOS DO CONTRATO DE ADESÃO. ÔNUS DA PROVA. INVERSÃO. POSSIBILIDADE TECNOLÓGICA DE COMPROVAÇÃO. CONFIGURADA. NÃO IMPLEMENTADA. TERMO GERAL DO CONTRATO DE MÚTUO. INEXISTÊNCIA. ELEMENTOS PROBANTES. AUSÊNCIA. DEVER DE REGISTRO DOS ATOS PRATICADOS. COMPROMISSO DE TRANSPARÊNCIA E DE INFORMAÇÃO. INCIDÊNCIA. CAPITALIZAÇÃO MENSAL DE JUROS. AUSÊNCIA DE PACTUAÇÃO EXPRESSA. VEDADA. SENTENÇA REFORMADA. MAJORAÇÃO DA SUCUMBÊNCIA. [...] 2. O contrato eletrônico é de mesma espécie do contrato tradicional, não se tratando de uma nova modalidade de contratação, divergindo apenas em sua forma, pois possui os mesmos requisitos para a sua validade jurídica. 3. O documento digital deve atender aos requisitos de identificação, autenticação, impedimento de rejeição, verificação e integridade, privacidade e aos princípios da neutralidade e da perenidade das normas reguladoras do ambiente digital, conservação e aplicação das normas jurídicas existentes aos contratos eletrônicos, boa-fé objetiva e figura do iniciador [...] (DISTRITO FEDERAL, 2017, documento *on-line*).

Tais requisitos estão relacionados com a capacidade das partes, a licitude do objeto do contrato e sua formalidade, de forma que o não atendimento a tais requisitos culmina em sua nulidade, ou seja, o contrato se torna um negócio jurídico inválido, que não faz lei entre as partes. Partindo dessa premissa, diversas são as ações envolvendo contratos eletrônicos no Brasil. Tais alegações dizem respeito tanto a questões individuais dos contratos eletrônicos — como validade da assinatura eletrônica e existência do certificado digital — quanto a questões triviais envolvendo contratos em geral — como validade e legitimidade das cláusulas. Para fins didáticos, aqui nos atentaremos somente às questões envolvendo as peculiaridades do contrato eletrônico, desprezando, portanto, assuntos acerca de contratos gerais.



Saiba mais

Em 2018, o Superior Tribunal de Justiça (STJ) julgou o Recurso Especial nº. 1.659.962 impetrado pela B2W Companhia Digital em face da apelação que condenou o grupo empresarial por danos materiais e morais por vender produtos pela internet e não fazer a entrega no prazo combinado, alegando não os ter em estoque. No caso, note que a lide versa sobre os termos do contrato e, portanto, o caso não se refere a, especificamente, contratos eletrônicos, mas sim à relação de consumo como um todo (BRASIL, 2018a).

Sobre os contratos eletrônicos, uma importante decisão proferida pelo STJ está relacionada com o reconhecimento da aludida corte acerca da validade de contratos digitais para a execução de dívidas. No ano de 2018, o STJ reconheceu ser possível a execução de dívida fundada em contrato eletrônico. Na ocasião, a parte que interpôs o Recurso Especial queria cobrar o devedor com base em um contrato eletrônico, mas teve o pedido negado pelo juiz de primeira instância. A justificativa para a negativa foi de que faltavam os requisitos do título executivo do documento, uma vez que não contava com assinatura de testemunhas. O entendimento foi reforçado pelo Tribunal de Justiça do Distrito Federal, que julgou a aludida apelação. O relator do caso, no STJ, em decisão inédita sobre o tema, permitiu a execução da dívida de forma direta pelo contrato digital, manifestando entendimento de que o contrato digital deveria ser equiparado aos contratos físicos, de papel. Para chegar a tal entendimento, o ministro Paulo de Tarso Sanseverino, relator do caso, entendeu que a legislação processualista civil brasileira exige apenas a existência de um documento para que haja a constituição do título executivo e que, nesse caso, enquadram-se os contratos eletrônicos, tendo em vista a autenticidade e veracidade atribuída à assinatura digital presente no documento. Para o relator, a ausência de testemunhas por si só não era capaz de afastar a legitimidade do documento e lembrou que “[...] grande parte dos negócios jurídicos não é mais celebrada em papel, mas em bites” (BRASIL, 2018b, documento *on-line*). Vejamos o inteiro teor do acórdão:

RECURSO ESPECIAL. CIVIL E PROCESSUAL CIVIL. EXECUÇÃO DE TÍTULO EXTRAJUDICIAL. EXECUTIVIDADE DE CONTRATO ELETRÔNICO DE MÚTUO ASSINADO DIGITALMENTE (CRIPTOGRAFIA ASSIMÉTRICA) EM CONFORMIDADE COM A INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA. TAXATIVIDADE DOS TÍTULOS EXECUTIVOS. POSSIBILIDADE, EM FACE DAS PECULIARIDADES DA CONSTITUIÇÃO DO CRÉDITO, DE SER EXCEPCIONADO O DISPOSTO NO ART. 585, INCISO II, DO CPC/73 (ART. 784, INCISO III, DO CPC/2015). QUANDO A EXISTÊNCIA E A HIGIEZ DO NEGÓCIO PUDEREM SER VERIFICADAS DE OUTRAS FORMAS, QUE NÃO MEDIANTE TESTEMUNHAS, RECONHECENDO-SE EXECUTIVIDADE AO CONTRATO ELETRÔNICO. PRECEDENTES. 1. Controvérsia acerca da condição de título executivo extrajudicial de contrato eletrônico de mútuo

celebrado sem a assinatura de duas testemunhas. 2. O rol de títulos executivos extrajudiciais, previsto na legislação federal em '*numerus clausus*', deve ser interpretado restritivamente, em conformidade com a orientação tranquila da jurisprudência desta Corte Superior. 3. Possibilidade, no entanto, de excepcional reconhecimento da executividade de determinados títulos (contratos eletrônicos) quando atendidos especiais requisitos, em face da nova realidade comercial com o intenso intercâmbio de bens e serviços em sede virtual. 4. Nem o Código Civil, nem o Código de Processo Civil, inclusive o de 2015, mostraram-se permeáveis à realidade negocial vigente e, especialmente, à revolução tecnológica que tem sido vivida no que toca aos modernos meios de celebração de negócios, que deixaram de se servir unicamente do papel, passando a se consubstanciar em meio eletrônico. 5. A assinatura digital de contrato eletrônico tem a vocação de certificar, através de terceiro desinteressado (autoridade certificadora), que determinado usuário de certa assinatura a utilizara e, assim, está efetivamente a firmar o documento eletrônico e a garantir serem os mesmos os dados do documento assinado que estão a ser sigilosamente enviados. 6. Em face destes novos instrumentos de verificação de autenticidade e presencialidade do contratante, possível o reconhecimento da executividade dos contratos eletrônicos. 7. Caso concreto em que o executado sequer fora citado para responder a execução, oportunidade em que poderá suscitar a defesa que entenda pertinente, inclusive acerca da regularidade formal do documento eletrônico, seja em exceção de pré-executividade, seja em sede de embargos à execução. 8. RECURSO ESPECIAL PROVIDO (BRASIL, 2018b, documento *on-line*).

Conclui-se, após todo o exposto, que, como derivado do meio eletrônico para concretização dos negócios jurídicos, os contratos eletrônicos trouxeram grandes avanços e desafios para o cenário atual, em virtude da celeridade, economia e facilidades advindas de tal modalidade. Entretanto, como consequência dessa nova realidade, surgem conflitos e preocupações. Cabe ao Poder Judiciário, com os entendimentos individualizados, estabelecer regramentos e regulamentos específicos para contratação em meio eletrônico, bem como moldar o que já existe de legislação no ordenamento jurídico brasileiro aos novos meios de comunicação, uma vez que a legislação aplicável aos contratos em geral é igualmente utilizada nas contratações eletrônicas, o que já garante segurança àqueles que se utilizarão desse meio de contratação para a realização de negócios jurídicos.

Referências

- BENJAMIN, A. H. V.; MARQUES, C. L.; BESSA, L. R. *Manual de direito do consumidor*. 3. ed. São Paulo: Revista dos Tribunais, 2010.
- BRANCHER, P. M. R. Contrato eletrônico. In: PUC-SP. *Enciclopédia jurídica da PUCSP*. São Paulo: PUC-SP, 2018. Disponível em: <https://enciclopediajuridica.pucsp.br/verbete/259/edicao-1/contrato-eletronico>. Acesso em: 17 abr. 2021.

BRASIL. *Lei nº 8.078, de 11 de setembro de 1990*. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em 02 abr. 2021.

BRASIL. *Lei nº 10.406, de 10 de janeiro de 2002*. Institui o Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 2 abr. 2021.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 1 abr. 2021.

BRASIL. *Medida provisória nº 2.200, de 28 de junho de 2001*. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, e dá outras providências. Brasília, DF: Presidência da República, 2001a. Disponível em: http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200.htm. Acesso em: 20 abr. 2021.

BRASIL. *Medida provisória nº 2.200-2, de 24 de agosto de 2001*. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Brasília, DF: Presidência da República, 2001b. Disponível em: http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm. Acesso em: 1 abr. 2021.

BRASIL. Superior Tribunal de Justiça. *Recurso especial nº 1.659.962 - RO*. Recorrente: B2W Companhia Digital. Recorridos: Emilia Simão de Souza, Rodolfo Scher da Silva. Relator: Min. Marco Buzzi, 5 de junho de 2018a. Disponível em: <https://stj.jusbrasil.com.br/jurisprudencia/589657258/recurso-especial-resp-1659962-ro-2017-0055468-1>. Acesso em: 2 abr. 2021.

BRASIL. Superior Tribunal de Justiça (3. Turma). *Recurso especial nº 1.495.920-DF*. Recorrente: Fundação dos Economistas Federais Funcef. Recorrido: Emerson Martineli Rodighiero. Relator: Min. Paulo de Tarso Sanseverino, 15 de maio de 2018b. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201402953009&dt_publicacao=07/06/2018. Acesso em: 1 abr. 2021.

CAVALIERI FILHO, S. *Programa de direito do consumidor*. 5. ed. São Paulo: Atlas, 2019.

DISTRITO FEDERAL. Tribunal de Justiça do Distrito Federal e dos Territórios (7. Turma). *Apelação Cível nº 20120111804179*. Apelante: Dirred Ali Husni. Apelado: Itaú Unibanco S.A. Relator: Des. Romeu Gonzaga Neiva, 19 de julho de 2017. Disponível em: <https://tj-df.jusbrasil.com.br/jurisprudencia/501193458/20120111804179-df-0049568-9320128070001/inteiro-teor-501193485>. Acesso em: 2 abr. 2021.



Fique atento

Os links para sites da web fornecidos neste capítulo foram todos testados, e seu funcionamento foi comprovado no momento da publicação do material. No entanto, a rede é extremamente dinâmica; suas páginas estão constantemente mudando de local e conteúdo. Assim, os editores declaram não ter qualquer responsabilidade sobre qualidade, precisão ou integridade das informações referidas em tais links.



editora
papervest

Publicação da Papervest Editora
Av. Marechal Floriano, 947 - CEP: 88503-190
Fone: (49) 3225-4114 - Lages / SC
www.unifacvest.edu.br