A ASSINATURA MANUSCRITA COMO DADO COMPORTAMENTAL À LUZ DA LGPD NA GESTÃO DOCUMENTAL DOS PROCESSOS PÚBLICOS E PRIVADOS

Mirna Schneider Braziolli de Oliveira[1]
Cristiane da Silva Oliveira[2]

RESUMO: *Este artigo propõe uma análise crítica e interdisciplinar sobre a assinatura manuscrita como dado sensível, a partir de uma abordagem que integra os aspectos comportamentais, legais e documentais no contexto da proteção de dados pessoais. Com base na Lei Geral de Proteção de Dados (Lei nº 13.709/2018), discutem-se os desafios enfrentados na gestão documental diante da necessidade de proteger elementos biométricos e de identidade comportamental, como a assinatura manuscrita. Em ambientes de gestão documental, públicos ou privados, isso apresenta um grande desafio: como garantir a integridade e a autenticidade dos documentos sem comprometer os direitos à privacidade e à proteção de dados? A partir de uma pesquisa teórica e legislativa, são apresentados os riscos, vulnerabilidades, implicações éticas e propostas de boas práticas para o tratamento adequado desse dado sensível no contexto organizacional.*

PALAVRAS-CHAVE: *Assinatura manuscrita; Grafoscopia; Proteção de dados; Dado biométrico; Gestão documental.*

INTRODUÇÃO

A assinatura manuscrita, tradicionalmente utilizada para autenticar e validar documentos passou a receber atenção especial no contexto da proteção de dados pessoais. Sendo o ato que formaliza um documento ou expressa consentimento, ela carrega, atualmente, uma complexidade que vai além de um simples traço no papel. Ela se transforma em uma verdadeira impressão digital comportamental, única para cada pessoa, fruto da delicada combinação entre os movimentos neuromotores e os processos cognitivos que ocorrem durante sua execução. Essa singularidade não apenas torna a assinatura praticamente impossível de ser imitada com precisão, como também a eleva a um status especial: o de dado biométrico sensível, protegido pela Lei Geral de Proteção de Dados, Lei nº 13.709/2018, (LGPD). Isso significa que seu uso, armazenamento e compartilhamento requerem cuidados rigorosos, seja no papel ou no ambiente digital.

1 Mirna Schneider é uma profissional multifacetada com carreira diversificada que abrange tecnologia, administração, comunicação e perícia grafotécnica, com especialização em proteção de dados e segurança cibernética. Possui Pós-Graduação em *Ethical Hacking* pela Faculdade Vincit e formação em Dados pela ESCOLA DNC, consolidando sua expertise técnica em análise, visualização e proteção de informações sensíveis. Desde 2023, atua na Secretaria Municipal de Urbanismo e Licenciamento (SMUL) da Prefeitura de São Paulo, onde trabalha diretamente com Integridade e Boas Práticas no Controle Interno, conduzindo projetos estratégicos voltados à conformidade com a LGPD (Lei Geral de Proteção de Dados) e implementação da LAI (Lei de Acesso à Informação).

2 Cristiane da Silva Oliveira é bibliotecária formada pelo Centro Universitário Leonardo da Vinci (UNIASSELVI – SP), com pós-graduação em Gestão Documental pela Gran Faculdades. Atua na área de gestão da informação e proteção de dados, com experiência em organização de acervos, controle documental e aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) no setor público. Atualmente, integra o setor de Controle Interno da Secretaria Municipal de Urbanismo e Licenciamento (SMUL) da Prefeitura de São Paulo, onde desempenha atividades relacionadas à Ouvidoria, gestão documental e conformidade com a LGPD.

Nesse contexto, a governança documental assume um papel estratégico crucial. Ela é responsável por assegurar que as assinaturas e os dados pessoais relacionados mantenham sua autenticidade, integridade e confidencialidade, requisitos indispensáveis para mitigar riscos, fortalecer a confiança dos cidadãos nas instituições e garantir a segurança jurídica, especialmente em um ambiente cada vez mais digital e, ao mesmo tempo, vulnerável a ameaças.

Sob a ótica técnica, a grafoscopia, o estudo científico das assinaturas, confirma que a assinatura é uma expressão dinâmica e única da interação entre o cérebro e os músculos, não um simples gesto mecânico que se repete facilmente. A incorporação dos dados dinâmicos amplia ainda mais o poder de validação, mas ressalta a necessidade de um esforço conjunto entre tecnologia, direito e gestão documental para proteger esses dados sensíveis.

Assim, a assinatura manuscrita permanece um elo essencial entre o mundo físico e o digital, carregando não apenas a identidade visual de quem a produz, mas também um conjunto singular de informações biométricas. Compreender essa complexidade é vital para proteger direitos individuais, assegurar a segurança jurídica e fortalecer a governança da informação em um cenário cada vez mais digitalizado e regulado.

O presente artigo busca investigar, sob uma perspectiva crítica e interdisciplinar, os desafios e as implicações legais, comportamentais e práticas da consideração da assinatura manuscrita como dado sensível, especialmente no âmbito da gestão documental. Considera-se, para tanto, a análise grafoscópica, a base legal da LGPD, os estudos da biometria comportamental e os princípios arquivísticos e de governança da informação. Este estudo, também, busca aprofundar essa compreensão, destacando a importância das práticas de proteção e governança documental como pilares para garantir a segurança, a autenticidade e a confiança nas relações documentais do presente e do futuro.

FIRMA, ASSINATURA E GRAFOSCOPIA

Para entendermos a firma ou assinatura como um valioso dado sensível, antes, precisamos conhecer um pouco sobre o exame do perito grafotécnico diante de uma suposta fraude. (NOTA: neste artigo não detalharemos os tipos de fraudes de assinaturas.)

Segundo Feuerharmel (2021, 3ª tiragem, p. 8):

> Firma é como um símbolo gráfico que representa formalmente uma determinada pessoa e é usada para autenticar documentos por ela emitidos, ou manifestar concordância com os termos de um assunto que lhe foi apresentado [...] Assinatura é uma firma produzida manualmente e usada como principal símbolo de autenticação pessoal.

Ao longo dos anos, cada pessoa desenvolve um padrão único de movimento ao assinar documentos, o que torna cada assinatura quase tão única quanto uma impressão digital.

> A assinatura possui um alto poder de identificação pessoal, algo amplamente discutido e validado por especialistas na área da escrita manual. Edmond Solange Pellat, considerado uma das maiores referências da Grafoscopia, desenvolveu quatro princípios científicos para explicar como a escrita se torna uma marca única de cada indivíduo. Dentre esses princípios, destaca-se especialmente aquele que afirma que o movimento gráfico é comandado diretamente pelo cérebro, mantendo suas características mesmo quando executado por uma mão funcional e adaptada à tarefa de escrever. (Pellat, 1927, p.11)

Esta lei estabelece que a escrita não é um ato puramente manual, mas sim um reflexo de comandos cerebrais complexos. O cérebro programa e coordena os movimentos finos necessários para a escrita, desenvolvendo um "automatismo gráfico" que é único para cada indivíduo. Assim, mesmo que a mão ou o instrumento de escrita variem, a essência do traçado reflete a "impressão" cerebral do escritor.

É o que vemos quando pessoas perdem os movimentos das mãos e passam a escrever com a boca ou os pés, mantendo as mesmas características gráficas.

Assim, a grafoscopia é a ciência que estuda os grafismos, ou seja, a escrita como marca pessoal. Dessa forma, é possível fazer o reconhecimento de uma determinada grafia por meio da comparação detalhada da letra. Isso permite identificar se uma assinatura é autêntica ou falsificada, por exemplo, o que torna a grafoscopia uma importante aliada nas estratégias antifraude.

FRAUDES EM ASSINATURAS

Com a digitalização crescente, documentos importantes também são assinados de maneira eletrônica. Embora as assinaturas digitais possam ser protegidas por certificados eletrônicos e outros mecanismos de segurança, ainda há uma grande quantidade de transações que dependem de assinaturas manuscritas.

Os processos em papel, tais como documentações de diferentes tipos de empréstimos, contratos e obtenção de subsídios no setor governamental, apresentam grandes problemas de segurança devido à dificuldade de manter o controle de acesso, à falta de trilhas de auditoria ou cadeia de custódia e ao risco de fraudes de assinaturas manuais.

É extremamente necessária a adoção de uma adequada gestão documental onde se tenha garantia de segurança de suporte da informação e, sobretudo, agilidade na sua recuperação e disseminação.

O uso de certificados e assinaturas digitais tem coibido um pouco esse risco, mas trouxe consigo outros desafios, que também não serão examinados neste artigo.

ASSINATURAS MANUSCRITAS EM SUPORTES DIGITAIS

Mas, o que dizer de assinaturas manuscritas em suportes digitais?

A assinatura eletrônica manuscrita ou, também conhecida como assinatura digital capturada – DCS, assinatura biométrica e assinatura grafométrica, combina a experiência natural das assinaturas tradicionais com os benefícios dos processos digitais.

A capacidade de individualização da assinatura manuscrita, mesmo em suportes digitais, ainda reside nos princípios fundamentais da grafoscopia: o automatismo gráfico e a manifestação de características psicomotoras únicas do indivíduo. A diferença principal é a forma como esses dados são capturados e os novos elementos que podem ser analisados.

Quando uma assinatura é feita em um *tablet*, smartphone ou mesa digitalizadora com uma caneta stylus ou o dedo, esses dispositivos são capazes de capturar muito mais do que apenas a imagem final da assinatura. Eles registram dados dinâmicos ou biométricos comportamentais, que são essenciais para a perícia grafotécnica digital.

Esses dados formam um "perfil biométrico" da assinatura, muito mais rico do que a simples imagem visual. Mesmo que a assinatura final pareça idêntica em formato, as características dinâmicas subjacentes podem revelar a autenticidade ou falsidade.

A PROTEÇÃO DE DADOS

Na LGPD o artigo 5º, inciso l, define dado pessoal como "informação relacionada à pessoa natural identificada ou identificável".

A identificabilidade de um dado pessoal não se limita apenas a informações que revelam diretamente o nome de um indivíduo. Ela abrange qualquer informação que, quando utilizada isoladamente ou em conjunto com outros dados disponíveis, possa levar à identificação, direta ou indireta, de uma pessoa natural.

O conceito de informação pessoal é a chave para entender o âmbito material da aplicação da Lei.

Também é informação de caráter pessoal aquela relativa à pessoa identificável; Os dados que potencialmente conduzem à individuação da pessoa são igualmente tomados como informação pessoal.

Existem dados ou identificadores que, apesar de não individualizarem efetivamente alguém, caso tratados com técnicas que são acessíveis e em conjunto com dados suplementares, podem levar à identificação de seu titular. Tomemos como exemplo o endereço IP.

Identificabilidade: Um endereço IP pode ser rastreado até um provedor de serviços de internet (ISP), que, por sua vez, possui os dados cadastrais do assinante daquela conexão em um determinado momento. Embora a identificação direta não seja imediata para o operador do website, a possibilidade de vinculação à pessoa natural por meio do ISP torna o endereço IP um dado pessoal identificável.

Da mesma forma, uma assinatura manuscrita quando associada a outros dados pode levar à identificação do indivíduo.

Em sequência, no artigo 5º, inciso ll, da LGPD é definido dado pessoal sensível como:

> Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. (BRASIL, 2018)

A LGPD foi criada para assegurar que o tratamento de dados pessoais ocorra respeitando os direitos fundamentais de privacidade e liberdade dos indivíduos. A lei está baseada em princípios essenciais, como a finalidade do uso dos dados, a adequação à finalidade proposta, a necessidade mínima de coleta e o dever de garantir a segurança da informação. Esses princípios, destacados em seu artigo 6º, orientam o tratamento de todos os dados pessoais, mas ganham ainda mais relevância quando se trata de dados sensíveis, devido ao seu potencial de causar discriminação ou danos ao titular.

Como vimos anteriormente, dada a evolução tecnológica, as assinaturas manuscritas são apostas em *tablets* ou mesas digitalizadoras que, por sua vez, além de fazerem a coleta da assinatura geram um perfil biométrico comportamental do indivíduo.

Os dados sensíveis, como a assinatura manuscrita quando vista sob o aspecto biométrico, recebem tratamento diferenciado pela LGPD. Conforme artigo 11, o uso desses dados exige consentimento específico, claro e destacado do titular, salvo em situações previstas em lei, como cumprimento de obrigação legal, execução de políticas públicas ou proteção da vida e da saúde. Essa exi-

gência visa evitar o uso indiscriminado e não autorizado de informações que podem revelar aspectos íntimos da pessoa, protegendo sua privacidade.

Além disso, a LGPD impõe às organizações a responsabilidade objetiva pelo tratamento adequado dos dados, por meio do princípio do *accountability* (prestação de contas). Isso implica que as instituições devem implementar políticas internas, controles técnicos, treinamento contínuo de funcionários e auditorias para garantir a proteção efetiva dos dados pessoais. Medidas como anonimização, criptografia e restrição de acesso são essenciais para mitigar riscos e garantir que a coleta e uso das assinaturas físicas, entre outros dados sensíveis, não gerem vulnerabilidades que comprometam os direitos dos titulares.

No artigo 5º da LGPD tanto o inciso l como o inciso ll podem ser aplicados às coletas de assinaturas, sejam em suportes físicos (papel) ou em suportes digitais, comprometendo os responsáveis pelo devido tratamento.

Até o momento não foram encontradas soluções para anonimização ou pseudo anonimização de assinaturas manuscritas em suportes físicos.

A ASSINATURA MANUSCRITA: DADO BIOMÉTRICO E COMPORTAMENTAL

A assinatura manuscrita permanece como uma expressão singular da identidade humana. Mais do que um traço gráfico sobre o papel, ela representa um dado biométrico de natureza comportamental, profundamente enraizado em fatores neuro motores, cognitivos e culturais. Em tempos de crescente digitalização e automatização dos sistemas de autenticação, a assinatura manuscrita continua a desempenhar papel central na validação de atos, contratos e na garantia de autenticidade documental, sobretudo em contextos jurídicos e administrativos.

De acordo com Freitas e Pimenta (2020), a assinatura manuscrita deve ser compreendida como uma manifestação gráfica pessoal, fruto de um conjunto de características motoras e mentais que se consolidam ao longo da vida do indivíduo. Trata-se, portanto, de um dado biométrico comportamental, ou seja, que depende de um gesto voluntário e de padrões dinâmicos que variam no tempo, como a pressão do traço, a velocidade de execução, a ordem dos movimentos e o ritmo de escrita. Tais elementos são involuntários e, por isso, de difícil reprodução ou falsificação por terceiros, o que confere à assinatura um elevado grau de individualização.

Diferente da biometria fisiológica, como impressões digitais, íris ou padrão facial, a biometria comportamental possui caráter dinâmico e contextual.

Como explica Rabelo e Rodrigues (2021):

> Enquanto a biometria fisiológica baseia-se em características anatômicas permanentes, a biometria comportamental exige a análise de como uma ação é executada, o que envolve memória muscular, estado emocional e cognição. Essa natureza torna a assinatura manuscrita particularmente útil em ambientes que exigem autenticação contínua ou periódica, como sistemas bancários, cartoriais e judiciais.

Do ponto de vista técnico, a assinatura manuscrita já é amplamente utilizada em sistemas de verificação automática, com aplicações em dispositivos móveis, caixas eletrônicos e plataformas digitais. Como destacam Lopes e Silva (2019), algoritmos baseados em inteligência artificial e redes neurais são capazes de captar e processar os chamados "bio traços" da escrita, como tempo de execução, inclinação, pressão e aceleração, para autenticar ou recusar uma assinatura com base em padrões previamente armazenados. Esses sistemas, ao integrarem variáveis comportamentais com parâmetros estatísticos e computacionais, ampliam o potencial da assinatura como ferramenta de segurança em meios digitais.

Sob uma perspectiva cultural e identitária, a assinatura manuscrita também exerce papel simbólico de autoria e intencionalidade. É um traço pessoal que acompanha o indivíduo desde a alfabetização, consolidando-se como elemento de representação social e jurídica. Como observa Torres (2018), a assinatura constitui um ritual de validação com valor probatório e afetivo, especialmente em atos solenes, contratos e manifestações de vontade. Seu uso transcende a funcionalidade técnica, integrando-se ao universo das práticas sociais de reconhecimento e legitimação.

Com a crescente digitalização dos processos e a adoção do assinador digital baseado em certificação ICP-Brasil, discute-se se a assinatura física se tornará obsoleta. Contudo, a prática mostra que ela continua sendo exigida em inúmeros contextos, tanto por sua acessibilidade quanto por seu valor jurídico. Além disso, a jurisprudência brasileira tem reconhecido a validade da assinatura manuscrita escaneada, desde que haja elementos complementares de autenticação, como CPF, número de documento e registro de IP, conforme decisões recentes dos tribunais.

Outro aspecto relevante é a utilização da assinatura física em perícias grafotécnicas, que continuam sendo fundamentais em processos cíveis e criminais. Como apontam Fernandes e Matos (2022), a análise forense da assinatura manuscrita ainda é um dos meios mais eficazes para detectar falsificações e fraudes em documentos, especialmente quando combinada com exames laboratoriais e análise de tinta, papel e cronologia de registros.

Por fim, é preciso destacar que a assinatura manuscrita, ao ser reconhecida como dado biométrico sensível, adquire uma nova centralidade no debate sobre proteção de dados, governança da informação e privacidade. Em tempos de

vigilância algorítmica e fluxos massivos de informação, preservar a segurança e o uso ético da assinatura é garantir também a dignidade e a autonomia do indivíduo frente às novas tecnologias.

Assim, reconhecer a assinatura física como dado biométrico comportamental não é apenas um exercício teórico, mas uma exigência prática de adaptação aos marcos regulatório, aos avanços tecnológicos e aos desafios contemporâneos da proteção da identidade. Ela permanece como símbolo de autenticidade, prova de intenção e expressão inerente da presença humana nos atos jurídicos e sociais. Trata-se, portanto, de um dado que deve ser protegido com o mesmo rigor com que se protegem as impressões digitais, a voz ou a imagem: com respeito, segurança e responsabilidade.

GESTÃO DOCUMENTAL E A DESAFIADORA INTERAÇÃO ENTRE A ASSINATURA MANUSCRITA E AS TECNOLOGIAS DIGITAIS

A sociedade atual vive uma era de transformação digital acelerada, que impacta todas as dimensões da vida pessoal à institucional, passando pelo ambiente corporativo. Nesse cenário dinâmico, as formas de produção, autenticação e armazenamento de documentos passaram por mudanças profundas, exigindo novas abordagens técnicas, jurídicas e gerenciais. Embora ainda detenha significativo valor simbólico e jurídico, a assinatura manuscrita vem sendo desafiada pelas transformações tecnológicas que remodelam os processos documentais e pela crescente exigência de conformidade com as normas de proteção de dados pessoais.

Dentro dessa realidade, a gestão documental emerge como um dos pilares da governança da informação, ao garantir a organização, o controle e a preservação dos documentos em todas as fases do seu ciclo de vida.

Como destaca Marilena Leite Paes (2004, p.53):

> A gestão documental deve ser compreendida como um “conjunto de procedimentos e operações técnicas referentes à produção, tramitação, uso, avaliação e arquivamento de documentos” que visa garantir a autenticidade, o valor informativo e o papel histórico dos documentos.

Quando se trata de documentos físicos assinados manualmente, a gestão deve assegurar a integridade e disponibilidade deste material, especialmente nos contextos jurídicos e administrativos. Isso requer políticas rigorosas de coleta, armazenamento, controle de acesso, rastreabilidade e descarte, respeitando tanto os princípios arquivísticos quanto os preceitos da LGPD. A especialista Luciana Duranti reforça que a autenticidade dos documentos, físicos ou digitais, depende de uma cadeia de custódia confiável, que inclui o contexto institucional, procedimentos formalizados e o uso de tecnologias adequadas. Diante

de um ambiente híbrido, em que documentos manuscritos são digitalizados para facilitar o acesso e a preservação, a responsabilidade é dupla: garantir o valor jurídico do original e proteger os dados pessoais ali contidos.

A assinatura manuscrita, por sua vez, carrega um significado histórico, jurídico e técnico que a torna indispensável em muitas situações. Ela demonstra claramente, o consentimento, o reconhecimento ou a autorização de um indivíduo, sendo considerada essencial para a validade de contratos, autorizações e diversos atos formais. No Brasil, a jurisprudência confere a essa assinatura a presunção de autoria e intenção. Além disso, como vimos, tecnicamente ela é um dado pessoal sensível, uma vez que reflete traços biométricos únicos, como forma, pressão, ritmo e inclinação. Isso exige um tratamento especial, sobretudo no ambiente digital. A digitalização da assinatura não elimina sua importância; pelo contrário, impõe exigências ainda maiores em relação à sua proteção e integridade, incluindo o controle de acesso ao documento original e a adoção de sistemas que garantam auditoria e rastreabilidade.

A Lei Geral de Proteção de Dados (LGPD), promulgada em 2018, consolidou-se como um marco fundamental na proteção da privacidade e dos direitos dos cidadãos em relação aos seus dados pessoais. A assinatura manuscrita, por possibilitar a identificação do indivíduo e conter traços biométricos únicos, enquadra-se no conceito de dado pessoal previsto no artigo 5º da norma, estando, portanto, sujeita aos princípios legais como finalidade, adequação, necessidade, segurança, transparência e responsabilização. Diante disso, tanto a gestão documental quanto os setores jurídicos das instituições devem manter vigilância constante e criteriosa, uma vez que falhas no manuseio de documentos assinados manualmente podem acarretar infrações legais, sanções financeiras e prejuízos à imagem institucional.

Entre os principais desafios enfrentados na gestão da assinatura manuscrita sob a ótica da LGPD, destacam-se a coleta e o consentimento. A captação da assinatura deve respeitar a liberdade do titular e ser acompanhada de consentimento claro e documentado, especialmente se digitalizada para armazenamento em banco de dados. Em relação ao armazenamento, tanto físico quanto digital, a preservação da assinatura impõe cuidados específicos. Documentos físicos estão sujeitos a riscos como extravio, incêndios e desgaste natural ao longo do tempo. Já a digitalização oferece maior eficiência e agilidade, mas demanda medidas rigorosas para assegurar a integridade e a confidencialidade das informações, incluindo o uso de criptografia, sistemas de backup seguros e práticas adequadas de descarte dos dados digitais. No caso de compartilhamento interno ou com terceiros, é imprescindível que haja base legal e medidas de segurança, prevenindo qualquer exposição indevida. Além disso, a LGPD assegura aos titulares o direito de acessar, corrigir e até solicitar a exclusão de seus dados pessoais. Quando se trata de uma assinatura com valor jurídico, o desafio é equilibrar a proteção dos dados com a necessidade legal de sua preservação.

Essa desafiadora interação entre a assinatura manuscrita e as tecnologias digitais de autenticação, como as assinaturas eletrônicas e digitais previstas na Medida Provisória nº 2.200-2/2001 e no Decreto Federal nº 10.278/2020, exige uma abordagem integrada e estratégica. Assim, cabe à gestão documental criar processos híbridos, que protejam e preservem adequadamente a assinatura manuscrita, bem como sua digitalização, assegurando sua conformidade com a LGPD e prevenindo a exposição desnecessária de dados pessoais.

Dentro da diplomática contemporânea, conforme enfatiza Luciana Duranti:

> A autenticidade de um documento não reside apenas na presença física de uma assinatura, mas na existência de um sistema documental robusto, sustentado por contexto institucional, protocolos claros e infraestrutura tecnológica. A assinatura manuscrita, nesse sentido, deve estar inserida em uma cadeia de custódia que garanta sua autenticidade, integridade e confidencialidade. No universo arquivístico, ela é parte fundamental da evidência que legitima o documento, o que exige sua preservação conforme normas que levem em conta não apenas seu valor histórico e jurídico, mas também o respeito à privacidade e à proteção dos dados pessoais.

Para que a gestão da assinatura manuscrita esteja em conformidade com a LGPD, é essencial adotar medidas práticas como a implementação de políticas de privacidade específicas, a definição clara de prazos de retenção e descarte e a formalização de cláusulas contratuais com terceiros que lidem com documentos assinados. Além disso, é fundamental garantir total transparência aos titulares sobre o tratamento de suas assinaturas, fornecendo informações claras sobre seus direitos e os canais disponíveis para exercício desses direitos.

O futuro da assinatura manuscrita, no contexto da proteção de dados, está intrinsecamente ligado ao avanço da inteligência artificial e das tecnologias biométricas. Tais inovações permitirão um controle mais refinado, com mecanismos capazes de identificar fraudes, autenticar múltiplos fatores e aplicar padrões rigorosos de acesso. Contudo, essas soluções tecnológicas trazem consigo novos desafios regulatórios, exigindo que sejam utilizadas com responsabilidade, ética e transparência, de modo a respeitar os direitos dos titulares e evitar a utilização abusiva de dados sensíveis.

Mesmo diante da ascensão das assinaturas digitais, a assinatura manuscrita continua desempenhando um papel crucial no ecossistema documental e jurídico brasileiro. Sob a luz da LGPD, sua utilização demanda um olhar cuidadoso, que combine a preservação de sua validade com o respeito à privacidade dos indivíduos. A gestão documental precisa, portanto, unir aspectos técnicos, legais e humanos para criar estruturas eficazes, seguras e transparentes. O grande desafio é, assim, conciliar o respeito à tradição com as exigências contemporâneas de proteção de dados, construindo uma governança da informação que honre o passado, atenda ao presente e se projete de forma responsável para o futuro.

INTERFACES INTERDISCIPLINARES: DIREITO, ARQUIVOLOGIA E PSICOLOGIA

A análise da assinatura como dado sensível não pode ser feita de forma isolada, pois envolve múltiplas áreas do conhecimento que se complementam. No campo do Direito, por exemplo, a interpretação da Lei Geral de Proteção de Dados (LGPD) exige uma visão cuidadosa, que respeite princípios constitucionais como a dignidade da pessoa humana e a proteção da intimidade. Autores como Doneda (2021) e Oliveira (2022) têm ressaltado a importância de adotar uma postura preventiva, buscando minimizar riscos e evitar o uso inadequado desses dados.

Já na Arquivologia, o foco se volta para o manejo técnico dos documentos que contêm assinaturas manuscritas. Bellotto (2017) destaca que o trabalho arquivístico deve acompanhar todo o ciclo de vida dos documentos, aplicando critérios rigorosos para sua avaliação e preservação. É essencial lembrar que as assinaturas, por sua natureza sensível, demandam cuidados especiais para garantir sua integridade e evitar violações.

Do ponto de vista da Psicologia,, a assinatura é muito mais do que um simples traço; ela reflete características psicológicas e emocionais do indivíduo. Abreu e Silva (2018) apontam que fatores como estresse, doença ou até mesmo tentativas de dissimulação podem alterar a forma como a assinatura é produzida.

Assim, compreender a assinatura como dado sensível requer um olhar que integre Direito, Arquivologia e Psicologia, reconhecendo que cada uma dessas áreas oferece elementos essenciais para a proteção, preservação e interpretação adequada desse tipo de dado.

Anonimizar a assinatura manuscrita dentro de um documento físico, preservando sua autenticidade, é um desafio que exige equilíbrio entre proteção da identidade e manutenção da validade jurídica. Uma forma é substituir a assinatura visível por um código ou selo especial no documento, que funcione como uma “chave” para acessar a assinatura original guardada em um local seguro, com controle rigoroso de acesso. Por exemplo, a assinatura pode ser substituída por um código alfanumérico ou marca d’água física que remeta a um registro oficial, onde a assinatura original está armazenada sob controles de segurança e acesso restrito. Assim, o documento pode ser compartilhado sem expor diretamente a assinatura do responsável, protegendo sua identidade contra usos indevidos. Quando for necessário comprovar a autenticidade, basta consultar o registro oficial vinculado ao código, garantindo que a assinatura é verdadeira e que o documento não foi alterado. Dessa maneira, conseguimos proteger um dado tão sensível quanto a assinatura manuscrita, respeitando a privacidade da pessoa, sem abrir mão da segurança e da validade legal do documento. É um jeito inteligente de equilibrar proteção e confiança na gestão documental. Mantendo a confiabilidade e a validade jurídica do documento.

CONCLUSÃO

A análise da assinatura manuscrita sob a ótica da proteção de dados pessoais revela a complexidade e a relevância que esse elemento tradicional de autenticação documental assume no contexto contemporâneo da segurança da informação e da governança documental. A assinatura, longe de ser apenas um traço gráfico convencional, constitui um dado biométrico comportamental único, dotado de características neuromotoras e cognitivas que permitem a identificação irrefutável de seu titular. Tal singularidade a enquadra, de forma clara, como dado sensível nos termos da Lei Geral de Proteção de Dados (LGPD), impondo novas responsabilidades e cuidados quanto ao seu tratamento.

O aprofundamento no exame grafoscópico demonstra que a assinatura é mais que uma mera formalidade: é uma manifestação física do automatismo gráfico moldado pela interação entre o cérebro e o membro motor. Essa relação intrínseca entre mente e movimento assegura a autenticidade do gesto assinado, conferindo à assinatura uma dimensão pessoal e intransferível. Por sua vez, a evolução tecnológica, que introduz a assinatura manuscrita em suportes digitais, amplia o espectro das informações capturadas, agora enriquecidas por dados dinâmicos e biométricos comportamentais, o que exige ainda mais rigor e sofisticação nos processos de autenticação e na proteção desses dados.

Nesse cenário, a LGPD surge como um marco imprescindível para garantir que o tratamento das assinaturas, físicas ou digitais, respeitem os direitos fundamentais à privacidade e à liberdade, especialmente considerando o potencial impacto negativo decorrente do uso inadequado desses dados sensíveis. O princípio do consentimento explícito, aliado ao dever de responsabilidade objetiva das organizações (*accountability*), desafia instituições públicas e privadas a adotarem práticas eficazes de governança documental, que englobem políticas bem definidas, controles técnicos eficazes, treinamento constante e mecanismos de auditoria rigorosos.

Ademais, a gestão documental, ao se posicionar como elemento central da governança da informação, deve transcender o simples arquivamento, assumindo papel estratégico na mitigação dos riscos relacionados à autenticidade, integridade e confidencialidade das assinaturas e demais dados pessoais associados. Essa postura é fundamental para assegurar a conformidade legal e preservar a confiança dos indivíduos nas instituições, sobretudo em um momento em que a digitalização avança rapidamente, mas as vulnerabilidades continuam latentes.

Por fim, a assinatura manuscrita, apesar dos desafios impostos pelas transformações digitais e legais, permanece como um elo vital entre o mundo físico e o digital, carregando em seus traços não apenas a identidade visual do signatário, mas também um conjunto singular de informações biométricas comportamentais que exigem um tratamento diferenciado e sensível. Reconhecer

e respeitar essa complexidade é imperativo para garantir uma proteção efetiva dos direitos individuais, consolidando a assinatura não só como um instrumento jurídico, mas também como um dado pessoal que reflete a singularidade humana em sua dimensão mais técnica e ao mesmo tempo mais íntima.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO 15489-1:2006: informação e documentação – gestão de documentos – parte 1: conceitos e princípios. Rio de Janeiro: ABNT, 2006.

BIONI, Bruno; MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz. *Tratado de proteção de dados pessoais*. 2. ed. Rio de Janeiro: Forense, 2023.

BRASIL. Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Institui a Infraestrutura de Chaves Públicas Brasileiras – ICP-Brasil. Diário Oficial da União, seção 1, Brasília, DF, p. 24, 27 ago. 2001.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, seção 1, Brasília, DF, p. 1, 15 ago. 2018.

BRASIL. Decreto nº 10.278, de 18 de março de 2020. Regulamenta os requisitos técnicos para digitalização de documentos públicos e privados, para que estes tenham o mesmo valor jurídico e probatório dos documentos originais. Diário Oficial da União, seção 1, Brasília, DF, p. 1, 19 mar. 2020.

CAMURÇA, Lia Carolina Vasconcelos. *Sociedade de vigilância, direito à privacidade e proteção de dados pessoais: uma análise sobre a influência de técnicas de publicidade comportamental na internet no consumidor-usuário*. Fortaleza, 2020.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). *Diretrizes para a certificação de repositórios arquivísticos digitais confiáveis (RDC-Arq)*. Brasília, 2023. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/Diretrizes_certificacao_rdc_arq_2023_12_12.pdf. Acesso em: 25 maio 2025.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). Resolução nº 43, de 4 de setembro de 2020. Estabelece diretrizes para digitalização de documentos arquivísticos. Disponível em: https://www.gov.br/conarq. Acesso em: 20 maio 2025.

COSTA, Ramon Silva. Os direitos da personalidade frente à sociedade de vigilância: privacidade, proteção de dados e consentimento nas redes sociais. *Revista Brasileira de Direito Civil em Perspectiva, [S.l.], 2019*.

CRUZ, Alexa. Grafoscopia: entenda a ciência que verifica se uma assinatura foi falsificada. Idwall, 17 fev. 2020. Disponível em: https://blog.idwall.co/grafoscopia-entenda-o-que-e/. Acesso em: 5 jun. 2025.

DEL PICCHIA FILHO, José; DEL PICCHIA, Carlos. *Tratado de Documentoscopia: da falsidade documental à fraude ideológica*. 2. ed. São Paulo: Millennium Editora, 2005.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. ed. Rio de Janeiro: Forense, 2021.

DURANTI, Luciana. Diplomática contemporânea: reflexões sobre sua aplicabilidade na era digital. *Revista Informação & Informação,* Londrina, v. 22, n. 2, p. 321–336, 2017. Disponível em: https://ojs.uel.br/revistas/uel/index.php/informacao/article/view/24421. Acesso em: 18 maio 2025.

FEUERHARMEL, Samuel. *Análise grafoscópica de assinaturas*. 3. tiragem. Rio de Janeiro: Millenium Editora, 2021.

FÉLIX, Silva. *Tecnologia em corporações: um estudo da era da documentação digital na empresa Gama*. FATEC Americana/SP, 2010. (Citado por PICCOLI et al., 2007, p. 91).

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27001:2022 – segurança da informação, cibersegurança e proteção da privacidade – sistemas de gestão de segurança da informação – requisitos. Genebra: ISO, 2022.

MACHADO, Diego; DONEDA, Danilo. A regulação da criptografia no direito brasileiro. In: *Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudoanonimização de dados*. p. 99-125. Editora Thomson; 2019.

PAES, Marilena Leite. Arquivo: teoria e prática. 2. ed. Rio de Janeiro: FGV, 2004, p.53.

PELLAT, Edmond Solange. Les lois de l'écriture: Étude psychologique, physiologique et graphologique de l'écriture et de ses altérations. Paris: Éditions Payot, 1927.