Série Proteção de Dados

15

A REGULAMENTAÇÃO DA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

VEIRANO ADVOGADOS



Este é o décimo quinto capítulo da Série Proteção de Dados. Clique aqui para acessar o cap. 14.



Em 2023, a Lei Geral de Proteção de Dados (Lei nº 13.709 de 2018 ou "LGPD") completa 5 anos de sua publicação – agora também com a possibilidade de aplicação das sanções administrativas pela ANPD, que se estende desde agosto de 2021. A Autoridade Nacional de Proteção de Dados ("ANPD") tem atuado ativamente para fomentar a discussão e disseminar os conceitos, práticas e princípios de privacidade e proteção de dados, com a publicação de diversos materiais para conscientização e regulamentação da LGPD desde a sua criação.

O Veirano Advogados tem acompanhado e participado das discussões relacionadas a estes temas. Por isso, nosso time de Proteção de Dados & Privacidade preparou a **Série Proteção de Dados**, na qual serão realizadas publicações periódicas sobre diferentes temas relacionados à privacidade, trazendo não somente os conceitos da LGPD, mas também publicações da ANPD sobre o tema, considerações relevantes, dentre outros conteúdos.



Conforme mencionado nos episódios anteriores desta série, a LGPD estabelece princípios e diretrizes claras para a coleta, tratamento e compartilhamento/transferência de dados pessoais, contemplando os direitos dos titulares, as obrigações dos Agentes de Tratamento, do Encarregado, os parâmetros para segurança da informação, os requisitos para a Transferência Internacional de Dados e as instruções quanto à atuação da Autoridade Nacional de Proteção de Dados ("ANPD"), dentre outras questões.

Desde a entrada em vigor da LGPD, diversas iniciativas setoriais têm sido propostas pelo Poder Público e pela iniciativa privada visando à adequação de diferentes setores à legislação e, ainda, a proposição de normas específicas para garantir a proteção dos dados pessoais nos setores econômicos.

Em âmbito federal, destaca-se o Guia de Boas Práticas sobre a LGPD, publicado pelo Governo Federal ainda em agosto de 2020.

Outrossim, para além dos documentos e publicações da ANPD (e.g., Guias Orientativos, Manuais, Cartilhas, entre outros) e de Análises de Impacto Regulatório (AIRs), Consultas Públicas e Tomadas de Subsídios propostas pela Autoridade, foram editados e publicados, nos últimos anos, Portarias, Enunciados, Resoluções e, ainda, Notas Técnicas visando à regulamentação da proteção de dados pessoais em âmbito nacional.

Em razão do avanço no tema, em 2023 a ANPD divulgou o balanço de acompanhamento e execução da Agenda Regulatória referente aos anos 2021 e 2022, publicou a Agenda Regulatória para o biênio de 2023-2024 e aprovou, por meio da Resolução CD/ANPD nº 5 de 2023, a Agenda de Avaliação de Resultado Regulatório para o período 2023-2026, conferindo ampla transparência, visibilidade e eficiência às ações regulatórias, possibilitando a participação e o acompanhamento pela sociedade e trazendo maior segurança jurídica na relação com os agentes regulados.

Abrangência do tema em setores econômicos

Com o intuito de harmonizar as atividades das mais diversas indústrias com os princípios e obrigações previstos pela LGPD e promover uma cultura de respeito à privacidade e à segurança da informação, agentes reguladores de diversos setores econômicos, observadas as competências legais que lhes são atribuídas e, também as que são atribuídas à ANPD, vêm editando normas e diretrizes que têm por objetivo assegurar a proteção de dados pessoais, por meio de procedimentos específicos aplicáveis a cada setor.

Em paralelo, cumpre observar que o Poder Público tem incentivado a criação de conselhos consultivos compostos por especialistas do setor, organizações da sociedade civil e representantes do governo. Esses órgãos têm a responsabilidade de elaborar diretrizes setoriais específicas, adaptadas às particularidades de cada segmento, promovendo uma compreensão mais clara das obrigações legais e dos melhores métodos de conformidade.

Outrossim, tanto na esfera pública quanto na privada, identificam-se, dentre as boas práticas adotadas, (i) a promoção de ações de educação e capacitação, por meio de treinamentos e workshops para os agentes de diversos setores, com o objetivo de propiciar a efetiva adequação às normas de proteção de dados pessoais e disseminar uma cultura que observe as boas práticas; (ii) a edição de guias/manuais orientativos aos setores econômicos, entre outras.



Considerações às normas setoriais sobre proteção de dados pessoais e sua relevância

Setor de Telecomunicações

O setor de telecomunicações é regido por um quadro legal e normativo que visa à garantia da proteção dos dados pessoais e à preservação da privacidade dos usuários de serviços de telecomunicações.

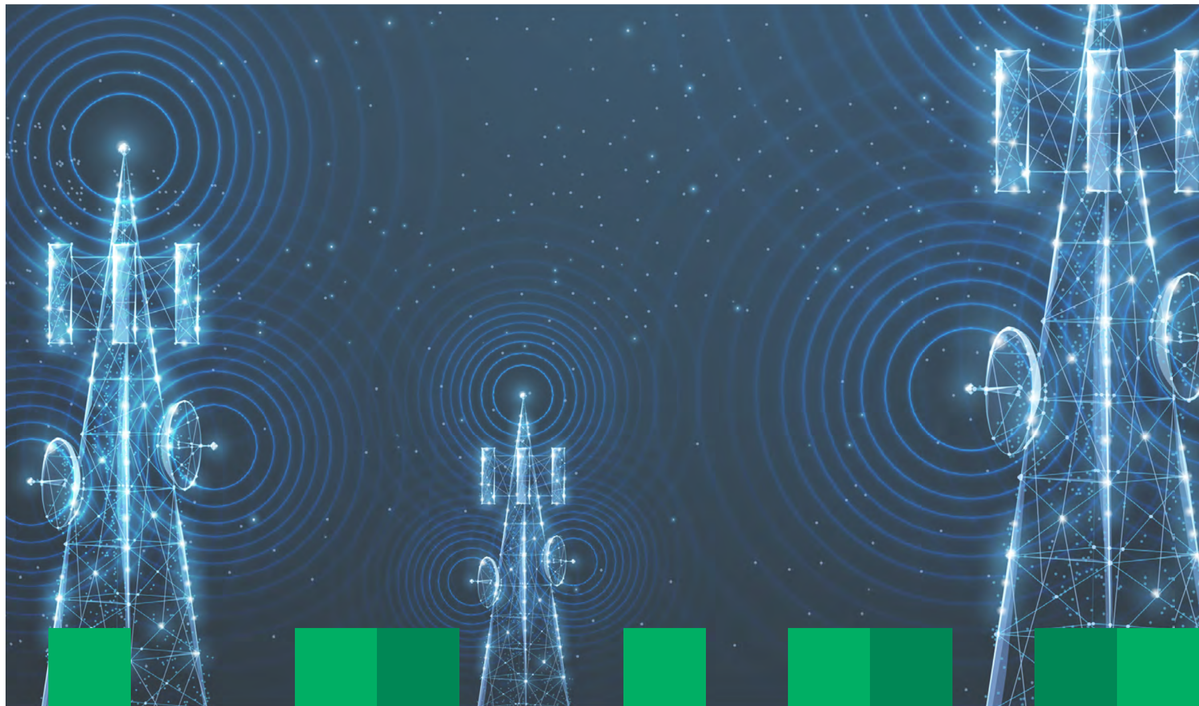
Nesse contexto, destacam-se a Lei Geral de Telecomunicações (Lei nº 9.472 de 1997 ou "LGT") e o Marco Civil da Internet (Lei nº 12. 965 de 2014 ou "MCI"), que estabelecem princípios e diretrizes para o tratamento de informações pessoais pelos agentes desse setor.

A LGT, particularmente, define (i) os direitos dos usuários, incluindo à privacidade de seus dados e ao sigilo das comunicações; (ii) os deveres e direitos dos provedores de serviços; e (iii) as diretrizes ao adequado tratamento destes dados pelos agentes.

Já o Marco Civil da Internet define os princípios e direitos no uso da Internet no país, dentre os quais a garantia à privacidade e à proteção de dados pessoais, excepcionados por requisição de divulgação por autoridade competente ou por ordem judicial que assim o determine.

Além das normas supramencionadas, o setor também é regulado por resoluções específicas, a exemplo do Regulamento Geral de Direitos do Consumidor de Serviços de Telecomunicações ("RGC"), aprovado pela Resolução nº 632 de 2014 da Agência Nacional de Telecomunicações ("ANATEL") e atualmente em revisão pela Agência, que trata de diversos aspectos dos direitos dos consumidores, incluindo a proteção de dados e privacidade, além de definir as regras para a coleta, armazenamento e tratamento de dados pessoais, exigindo que as empresas adotem práticas transparentes e seguras.

Já o Regulamento dos Serviços de Telecomunicações (aprovado pela Resolução nº 738 de 2020 da ANATEL) consiste em outra peça importante do quadro regulatório setorial, visto que, alinhando-se com a LGPD, estabelece às empresas de telecomunicações o dever de reter a menor quantidade possível



de dados de usuários, mantendo-os sob sigilo, em ambiente controlado e de segurança, observados os recursos tecnológicos necessários à suspensão do sigilo e excluindo os dados tão logo atingida a finalidade de seu tratamento ou quando encerrado o prazo de guarda determinado por obrigação legal ou regulatória. Além disso, o Regulamento dispõe, de forma abrangente, sobre a guarda de dados pessoais para fins de atendimento de obrigações legais e regulatórias pelas prestadoras de serviços de telecomunicações, conferindo maior segurança jurídica ao tratamento realizado pelos agentes.

Nos últimos anos, diante da crescente substituição do serviço fixo pelo móvel e, dos diferentes regimes a eles conferidos, oriunda da mudança comportamental dos usuários de serviços de telecomunicações e do avanço tecnológico e da consolidação de novos modelos de serviços, vem crescendo a relevância dos dados e os impactos do tratamento de dados.

Percebe-se, portanto, que as normas regulamentadoras atuam em conjunto na salvaguarda da inovação e dos direitos dos indivíduos, enquanto titulares de dados pessoais, promovendo a transparência, a segurança e a confiança no ambiente digital.

Em linha com o ora apresentado, em recente auditoria realizada pelo Tribunal de Contas da União, fruto do Acórdão 1384 de 2022-TCU-Plenário que aprovou o processo de auditoria realizada em 382 organizações públicas federais para avaliar a aderência de suas ações às diretrizes estabelecidas pela Lei Geral de Proteção de Dados, a ANATEL obteve, de acordo com o Relatório, 0,76 no indicador de adequação à LGPD, demonstrando se encontrar em um nível "intermediário" de adequação.



Setor de saúde suplementar

O setor de saúde suplementar é considerado altamente sensível quando se trata da proteção de dados pessoais, dado o potencial impacto na privacidade e na intimidade dos indivíduos/titulares de dados pessoais. Isso se deve, em grande parte, ao volume de informações e dados sensíveis (e.g., informações médicas, históricos de tratamentos, exames clínicos e condições de saúde) que são coletados, tratados e retidos por instituições de saúde, como clínicas, hospitais e empresas farmacêuticas, e seus profissionais.

Além disso, o tratamento de dados no âmbito do setor de saúde está intrinsecamente ligado ao benefício conferido pelos serviços e produtos ofertados. É dizer, no contexto da oferta de serviços e produtos no setor de saúde, a coleta e o tratamento adequados desses dados são medidas cruciais para fins de personalização de tratamentos, prevenção e combate a doenças e eficácia dos cuidados médicos. Além disso, são essenciais para o desenvolvimento de novos medicamentos e terapias.



A LGPD estabelece importantes diretrizes para a coleta, uso e tratamento de dados pessoais sensíveis, que incluem dados genéticos e aqueles referentes à saúde e à vida sexual, reconhecendo a relevância dessas informações e a necessidade de protegê-las de maneira rigorosa. Os dados pessoais sensíveis englobam informações que, se mal utilizadas ou expostas, podem causar danos significativos à privacidade e à dignidade dos titulares.

Ainda sobre o tema foi promulgada a Lei nº 14.510, de 2022, que autoriza e disciplina a prática da tele saúde em todo o território nacional e o Conselho Federal de Medicina (CFM) publicou a Resolução nº 2.314 de 2022, que define e regulamenta a telemedicina para fins de assistência, educação, pesquisa, prevenção de doenças e lesões, gestão e promoção de saúde.

De acordo com a norma, a prestação de serviço de telemedicina, deverá seguir os padrões normativos e éticos usuais do atendimento presencial, e o atendimento deve ser precedido de consentimento explícito, no qual o paciente ou seu representante legal deve estar consciente sobre a possibilidade de seus dados pessoais serem compartilhados, bem como sobre seu direito de revogar o consentimento, salvo em situação de emergência médica.

Outrossim, nos serviços prestados por telemedicina, os dados e imagens dos pacientes constantes no registro do prontuário devem ser preservados, obedecendo as normas legais e aquelas editadas pelo CFM pertinentes à guarda, ao manuseio, à integridade, à veracidade, à confidencialidade, à privacidade, à irrefutabilidade e à garantia do sigilo profissional das informações.

Outro aspecto relevante é a interoperabilidade dos sistemas de saúde, que permite a troca de informações entre diferentes entidades, mas exige um cuidado especial com a proteção dos dados durante esse processo.

A sensibilidade do tema ressalta a necessidade de uma abordagem cuidadosa e ética na coleta, armazenamento e compartilhamento de informações médicas, a fim de preservar a dignidade e os direitos dos indivíduos, ao mesmo tempo em que permite avanços significativos na prestação de serviços de saúde.

Não por outro motivo, a iniciativa privada vem coordenando iniciativas de autorregulação, a exemplo do Código de Boas Práticas - CNSAúde (Confederação Nacional de Saúde), que traz uma compilação de orientações a serem observadas pelos agentes de saúde. O Código aborda aspectos como a transparência na coleta de dados, a obtenção de consentimento adequado dos titulares de dados pessoais, a adoção de medidas de segurança robustas para prevenir vazamentos e ataques cibernéticos, além de diretrizes para o compartilhamento seguro entre profissionais de saúde.

Na mesma toada, a Cartilha elaborada pelo Instituto Brasileiro de Defesa do Consumidor (IDEC) apresenta um panorama sobre a proteção de dados no contexto do setor da saúde e aborda temas como o direito à saúde, a transformação digital, o uso de dados pessoais no acesso a medicamentos e serviços de saúde e desafios apresentados pela Inteligência Artificial. Ainda de acordo com o Instituto, as políticas de uso de dados encontram-se em fase de construção no Brasil e no mundo, mas já há preocupações específicas no setor da saúde.

Por sua vez, a Agência Nacional de Saúde Suplementar (ANS) vem desempenhando um papel fundamental na regulamentação do tema. Dentre as iniciativas da Agência, destaca-se a Cartilha de Proteção de Dados Pessoais, que tem um papel categórico na orientação de agentes de saúde, profissionais do setor e pacientes sobre as melhores práticas para proteção de dados pessoais. Com efeito, a Cartilha aborda temas como a necessidade de transparência na coleta e no tratamento dos dados, os direitos dos titulares, a importância da segurança da informação e da adoção de medidas técnicas e organizacionais adequadas para evitar o acesso não autorizado, vazamentos e outros incidentes de segurança, dentre outros.

Por fim, desde 2022, a atuação da ANS vem sendo orientada, dentre outras, pela Resolução nº 80, de 28 de junho de 2022, que dispõe sobre a Política de Proteção de Dados Pessoais no âmbito da Agência.



Setor de aviação civil

O tratamento de dados pessoais é crucial para o desenvolvimento e modernização do setor de aviação civil. A coleta e análise de dados pessoais de passageiros, tripulantes e outros agentes são essenciais para atender às normas aplicáveis e garantir um alto padrão de segurança, eficiência e conveniência das operações aéreas. Nesse sentido, as companhias aéreas e as autoridades de aviação utilizam dados pessoais para verificações de histórico, identificação de passageiros e tripulantes, e garantir a conformidade com os regulamentos de segurança e imigração.

Outrossim, o uso de dados pessoais permite, por exemplo, às companhias aéreas e autoridades de aviação entenderem melhor as necessidades dos passageiros com deficiência, tornando possível a adaptação de serviços e instalações para atender a essas demandas específicas, à luz das normas de acessibilidade.

Além disso, o uso de dados pessoais é importante para melhorar a experiência do passageiro. As companhias aéreas usam dados para personalizar serviços, disponibilizar ofertas especiais com base nas preferências dos passageiros e melhorar a eficiência das operações, como o embarque e desembarque, preferências de assentos e refeições especiais. Isso contribui para uma experiência mais agradável e conveniente para os viajantes, e ajuda as companhias aéreas a otimizarem suas operações e alocarem recursos de forma mais eficaz.

No entanto, a relevância do uso dessas informações na aviação civil também levanta questões importantes sobre a privacidade e a proteção de dados, tendo em vista o alto volume e contínuo fluxo de dados pessoais e pessoais sensíveis.



No âmbito da Agência Nacional de Aviação Civil ("ANAC"), ainda em 2015, foi publicado o Manual de Tratamento de Informações com Restrição de Acesso, que em seu item 3.2. trata das informações consideradas como pessoais e/ou sensíveis e do respeito à intimidade e à vida privada conferido aos titulares destes dados.

Após a entrada em vigor da LGPD, a Agência aprovou, por meio da Instrução Normativa nº 172, de agosto de 2021, a Política de Proteção de Dados Pessoais da ANAC, assegurando a conformidade do tratamento com a legislação de proteção de dados. Também foram publicados o Aviso de Privacidade da ANAC e a Portaria nº 2.235, de agosto de 2020, que designa o Encarregado pelo Tratamento de Dados Pessoais no âmbito da Agência.

Em recente auditoria realizada pelo Tribunal de Contas da União para diagnóstico acerca dos controles implementados pelas organizações públicas federais para adequação à LGPD, verificou-se, pelo Relatório que a ANAC obteve o valor de 0,48 para o indicador de adequação à LGPD, o que corresponde ao nível "inicial".

Ainda sob a ótica de boas práticas, importa observar que a ANAC possui uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), criada pela Portaria nº 9.367 de STI, com a atribuição de receber, analisar e responder às notificações referentes a incidentes de segurança, bem como atuar de maneira preventiva para reduzir o risco e o impacto de possíveis incidentes de segurança da informação.



Setor de transportes aquaviários

A coleta e análise de dados pessoais, como informações dos passageiros e tripulantes, permitem às autoridades marítimas e às empresas de transporte monitorar e garantir a conformidade com regulamentações de segurança, como verificações de antecedentes e controle de acesso a áreas sensíveis em embarcações. Isso é essencial para prevenir ameaças à segurança, como pirataria e atividades ilícitas.

Além disso, a utilização de dados pessoais também é crucial para melhorar a experiência dos passageiros/titulares de dados pessoais, visto que as empresas de transporte aquaviário podem usar informações sobre preferências, histórico de viagens e feedback dos passageiros para personalizar serviços, como cardápios, entretenimento a bordo e acomodações, atraindo mais clientes e aumentando sua competitividade no mercado.

Outrossim, o uso de dados pessoais permite que os agentes regulados identifiquem padrões de demanda, comportamento do consumidor e eficiência operacional. Isso permite que eles ajustem suas operações, horários e rotas para atender às demandas de forma mais eficaz, reduzindo custos e melhorando a qualidade do serviço.

A Agência Nacional de Transportes Aquaviários (“ANTAQ”) aprovou a Política de Proteção de Dados Pessoais (PPDP), por meio da Portaria DG ANTAQ nº 425 de 2022. A PPDP se aplica a todos que, de forma direta ou indireta, realizem atividades que envolvam o tratamento de dados pessoais custodiados pela agência. A PPDP estabelece diretrizes claras e abrangentes para a gestão e proteção de dados pessoais no âmbito da ANTAQ, abordando aspectos como coleta, armazenamento, tratamento e compartilhamento de informações pessoais em conformidade com as disposições LGPD no contexto das atividades da Agência.

Além disso, a ANTAQ tem buscado alinhar-se às normas e diretrizes setoriais, como evidenciado pelo Relatório de Feedback do TCU, que, ao analisar o empenho da agência em adaptar suas práticas operacionais e estratégicas para garantir a segurança e a privacidade dos dados pessoais, conferiu 0,60 no indicador de adequação à LGPD, valor este correspondente ao nível intermediário de adequação às normas de proteção de dados pessoais.

Setor de Transportes Terrestres

Particularmente no âmbito do setor de transportes terrestres, o tratamento de dados pessoais, realizado pelo Poder Público (inclusive a ANTT) e pelos agentes regulados, tem por objetivo principal assegurar aos usuários adequadas infraestrutura e prestação de serviços de transporte terrestre, com transparência e regulação efetiva, proporcionando a melhoria contínua dos serviços ofertados. Para tanto, são tratados dados pessoais relacionados (i) aos passageiros de transporte rodoviário e, sempre que cabível, ferroviário; (ii) aos transportadores pessoas físicas, a exemplo daqueles constantes no Cadastro Nacional dos Transportadores Rodoviários de Mercadorias; e (iii) prestadores de serviços ou fornecedores.

Diante disso, foi publicado pela CNT/SESTSENAT/ITL, em parceria com representantes dos diversos modais, o "Guia de Boas Práticas de Proteção de Dados no Setor de Transporte", que visa a estabelecer padrões e protocolos para o tratamento de dados pessoais, facilitando e otimizando a adequação e a aplicação da normativa relacionada ao tema pelas empresas do setor.

No contexto atual da ANTT, a despeito das iniciativas ainda serem incipientes, o Conselho Diretor, por meio da Deliberação nº 448 de 2020 instituiu a Comissão de Apoio à Proteção de Dados Pessoais, que tem por objetivo formular diretrizes relacionadas à LGPD, bem como dar suporta na elaboração de procedimentos e protocolos internos para ações de tratamento de dados pessoais e proteção à privacidade.

Outrossim, de acordo com o Aviso de Privacidade da Agência, a autarquia está em processo de adequação aos normativos legais que dispõem sobre proteção de dados. Neste contexto se insere a publicação de manuais e guias, bem como a constituição de comitês voltados ao tema.



Setor financeiro e de meios de pagamento

Antes mesmo da LGPD, já havia normas específicas que prezavam pelo sigilo e confidencialidade do tratamento e armazenamento de dados e informações pessoais realizados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central. Como exemplo, destaca-se a Lei Complementar nº 105 de 2001 ("Lei do Sigilo Bancário"), que assegura a confidencialidade dos dados financeiros, salvo por ordem judicial que determine a disponibilização para fins de apuração ou investigação de atos ilegais.

Referido normativo tem como objetivo preservar a privacidade relacionada às atividades bancárias, bem como contempla regras que objetivam evitar práticas ilícitas.

Outro exemplo é a Resolução BACEN nº 4.658 de 2018, revogada pela Resolução CMN nº 4.893 de 2021, que dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de tratamento/processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.

Em um setor cujas operações envolvem procedimentos, pessoas, programas, equipamentos, normas internas e normas legais, a arquitetura desse sistema deve observar múltiplos aspectos da proteção de dados pessoais e da



privacidade (e.g., controle de acesso, rastreabilidade, conhecimento das finalidades declaradas e executadas, anonimização de dados, entre outros).

Não à toa, a proteção de dados pessoais tem se mostrado elemento intrínseco à adequada atuação no setor, na medida em que o devido tratamento destes dados pessoais, a segurança e a gestão da informação desempenham papel fundamental nas operações financeiras. Com a digitalização dos serviços ofertados, a implementação de uma cultura voltada à proteção de dados pessoais vem se mostrando medida cada vez mais urgente para todos os agentes.

Com a entrada em vigor da LGPD, novas diretrizes e obrigações foram introduzidas, visando à proteção ao crédito por meio de uma abordagem regulatória com traços de inovação.

Embora o dado financeiro ou bancário não integre o rol taxativo dos dados pessoais sensíveis previstos na LGPD, tal como se verifica no artigo 9º do GDPR, os riscos resultantes de eventual incidente de segurança vêm sendo

reconhecidos no âmbito sancionatório e, por conseguinte, inaugurando novas preocupações quanto à sua proteção, na medida em que a correlação entre sigilo de dados financeiros e a proteção à intimidade e à privacidade tem o condão de justificar a adoção de cuidados técnicos robustos.

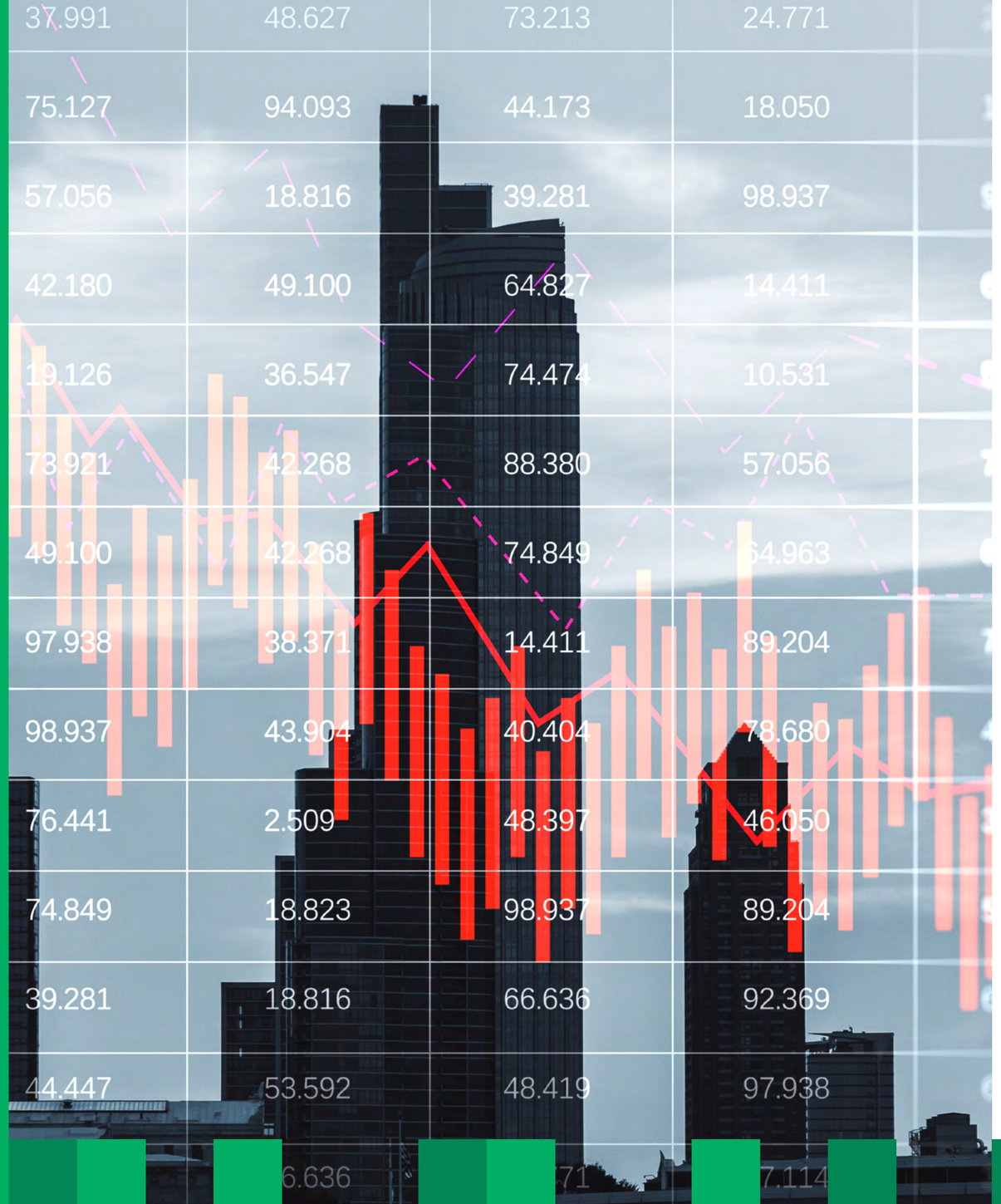
Nos últimos anos, o setor tem experimentado uma evolução tecnológica e mercadológica significativa, em grande parte proporcionada por uma regulamentação pró-competitiva.

A título exemplificativo, cita-se a regulamentação do *Open Finance* (inicialmente referida como *Open Banking*), que busca facilitar o compartilhamento de dados e serviços por meio de um sistema aberto e interoperável mediante o empoderamento do titular dos dados. Trata-se de um ótimo exemplo das inovações que vêm sendo introduzidas neste segmento.

O tema foi objeto de ampla discussão e posteriormente regulamentado por meio da Resolução Conjunta nº 01 de 2020, cujo texto já foi alterado por outras normas. Nessa linha, a Resolução Conjunta nº 05 de 2022, que introduziu importantes alterações na regulamentação em questão, definiu a interoperabilidade como sendo "*o compartilhamento padronizado de dados, mediante consentimento de cliente, de forma segura, ágil e precisa, entre os participantes dos sistemas disciplinados (...)*", com o fito de (i) estimular a inovação; (ii) promover a concorrência; (iii) aumentar a eficiência do Sistema Financeiro Nacional e do Sistema de Pagamentos Brasileiros e; (iv) promover a cidadania financeira.

Ocorre que a segurança dos dados tem sido uma preocupação na implementação do *Open Finance*, que requer a adoção de medidas efetivas de proteção dos dados pessoais dos titulares, sobretudo considerando que a





interoperabilidade dos sistemas poderá acarretar um expressivo aumento no volume de compartilhamentos – sendo certo que a confiança do usuário na segurança das informações é imprescindível para o sucesso da iniciativa.

Cabe citar também a Resolução Conjunta nº 6, de 2023, que entrará em vigor a partir de 1º de novembro de 2023, e que estabelece requisitos para o compartilhamento de dados e informações sobre indícios de fraudes, a serem observados por instituições financeiras, instituições de pagamento e demais instituições autorizadas a funcionar pelo Banco Central. Destaca-se, nesse sentido, a obrigação de obtenção de consentimento prévio dos titulares para o registro de dados e informações em seus sistemas (salvo dados e informações sigilosos, nos termos de legislação especial, relacionados a indícios da prática dos crimes de "lavagem" ou ocultação de bens, direitos e valores e de financiamento do terrorismo).

Em tempo, após a entrada em vigor da LGPD, nota-se que o BACEN publicou sua Política de Privacidade e aprovou, por meio da Resolução BCB nº 249, de 2022, sua Política de Governança da Informação, aplicável ao tratamento de qualquer informação em meio digital, físico ou oriunda de comunicações que sejam recebidas, coletadas e tratadas pelo Banco Central, e que visa, dentre outros objetivos, à proteção das informações tratadas pelo regulador, garantir a disponibilidade e a qualidade adequada das informações básicas para o cumprimento das missões institucionais, garantir a devida prestação de informações à sociedade, em especial as de interesse público, e o compartilhamento de informações com outros órgãos público.

Outros setores

Cumpre destacar também os esforços que vêm sendo empreendidos por outras Agências Reguladoras (e.g., ANA, ANCINE e ANEEL), que apesar de não terem editado normas especificas relacionadas relacionada ao tema, vêm inaugurando iniciativas de adequação do setor à legislação de proteção de dados pessoais.

Da Defesa da Concorrência

Tendo em vista a crescente importância dos dados para a atuação em diversos mercados, sobretudo com o advento da Economia Digital, nota-se cada vez mais uma interseção entre o tema com a defesa da concorrência. Há diversos exemplos de investigações conduzidas pela autoridade concorrencial em que a principal variável (ou uma das principais variáveis) é (ou foi) a detenção de dados por parte de um ou poucos agentes econômicos, a reduzida replicabilidade de tais informações, e a possibilidade de se cometer abuso a partir disso.

Nessa esteira, é inegável que a LGPD possui um aspecto concorrencial em suas determinações, estabelecendo a livre concorrência como um de seus fundamentos. Nesse contexto, o Conselho Administrativo de Defesa Econômica ("CADE") e a ANPD firmaram, em junho de 2021, Acordo de Cooperação Técnica para o aperfeiçoamento das ações voltadas à defesa, fomento e disseminação da concorrência no âmbito dos serviços de proteção de dados.



Em síntese, a finalidade do acordo é instituir uma cooperação técnica entre as autoridades para viabilizar ações conjuntas e coordenadas quando da ocorrência de situações que tocam matérias de suas competências, contribuindo para o combate às atividades lesivas à ordem econômica e para o fomento e disseminação da cultura da livre concorrência. Para tanto, define obrigações comuns (como compartilhamento de documentos, estudos e pesquisas, informações, conhecimentos e experiências, realização de reuniões, promoção de seminários, produção de estudos) e obrigações para cada uma delas – inclusive, no caso do CADE, comunicar à ANPD a respeito de instauração de investigação em desfavor de agentes econômicos que atuem em setores regulados pela ANPD; e, no caso da ANPD, comunicar ao CADE sobre instauração de investigação que porventura possa tipificar infração à ordem econômica.

Na mesma ocasião, o CADE divulgou o trabalho "***Benchmarking internacional sobre as instituições de Defesa da Concorrência e de Proteção de Dados***", contendo análise sobre as instituições de proteção de dados e de defesa da concorrência de doze jurisdições, além do Brasil.

Desafios

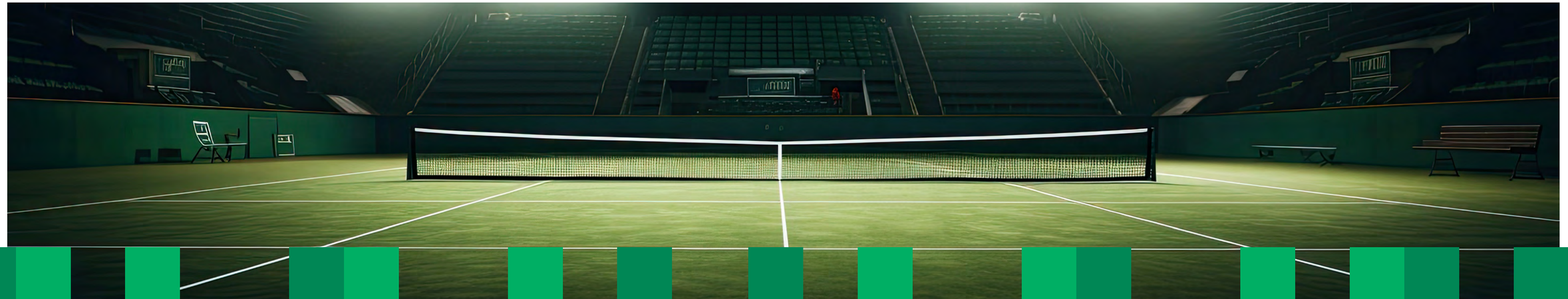
A edição de normas específicas de proteção de dados para cada setor econômico, embora seja em parte necessária devido às particularidades de cada área, vem resultando em um mosaico de regras e diretrizes com desafios significativos de harmonização e interpretação sistemática.

Os desafios de harmonização e coordenação residem, principalmente nas especificidades regulatórias de cada setor, visto que cada um possui características únicas (e.g., diversidade de interesses, tecnologias e práticas) em relação à importância e ao volume de dados pessoais que são, dentre de suas dinâmicas particulares, coletados e tratados.

Além disso, em uma sociedade em que a evolução tecnológica ocorre de maneira rápida e os dados, sobretudo em mercados digitais, podem revelar como os indivíduos pensam, decidem e consomem, configurando verdadeiros ativos e estabelecendo novas dinâmicas nas relações sociais, desponta a necessidade de um acompanhamento periódico dos agentes reguladores, responsáveis por regular novas tecnologias e rever as normas vigentes, e acrescenta-se um nível adicional à complexidade de harmonização de normas sobre proteção de dados pessoais.

Soma-se a isso a existência de iniciativas legislativas que visam a aprimorar, direta ou indiretamente, a proteção de dados pessoais, bem como regular o uso de inteligência artificial no país, evidenciando a importância de uma atuação colaborativa e conjunta entre o poder legislativo, os órgãos reguladores e os agentes regulados.

Contudo, apesar dos desafios mencionados, é crucial que os reguladores busquem um equilíbrio entre a especificidade necessária para cada setor e a necessidade de consistência e clareza nas regras de proteção de dados, em prol do desenvolvimento econômico do país. Com efeito, para grupos que operam em múltiplos setores, por exemplo, a conformidade com um mosaico de regulamentações complexas pode se tornar medida desafiadora e onerosa, dificultando a implementação de práticas de forma coesa e eficiente.



Por outro lado, a convergência entre essas normas traz diversos benefícios.

» **Em primeiro lugar**, ela não apenas reduz a carga administrativa e minimiza contradições e lacunas normativas, mas também permite que os agentes regulados atuem em maior conformidade com o arcabouço legal e normativo de proteção de dados pessoais. Com isso, os agentes econômicos são capazes de desenvolver sistemas e processos internos que se alinham de maneira mais direta com as regulamentações, garantindo uma abordagem mais sólida e abrangente e minimizando impactos operacionais.

» **Em segundo lugar**, a segurança jurídica oriunda da harmonização entre normas setoriais tende a acarretar maior confiança entre os agentes que integram as cadeias de serviços. Isso porque ao perceberem que suas informações e dados pessoais estão sendo tratados adequadamente, independentemente do setor de atividade, estes podem ficar mais propensos a permitir o compartilhamento de seus dados pessoais.
Ademais, ao respeitar as regulamentações de proteção de dados em todos os setores em que operam, os agentes regulados demonstram seu compromisso com a privacidade e a integridade dos dados pessoais, fortalecendo a confiança entre estes e terceiros e promovendo uma cultura de respeito à privacidade.

» **Em terceiro lugar,** a afinidade entre as normas setoriais também promove maior clareza e transparência, mitigando preocupações com a segurança da informação. É dizer, a eficácia das normas de proteção de dados pessoais também é amplificada quando os atores conseguem adotar medidas preventivas abrangentes.

» **Em quarto lugar**, a harmonização é benéfica para a cooperação interdisciplinar. Frequentemente, para o desenvolvimento e a implementação de modelos de negócio, agentes econômicos de distintos setores precisam compartilhar dados pessoais. Nesse cenário, o emprego de normas que possibilitem uma interpretação sistemática facilitaria o adequado tratamento e compartilhamento destes dados.

» **Finalmente**, diante de uma maior coesão entre as normas regulamentadoras, o poder público, assim como a iniciativa privada, encontra maior facilidade em desenvolver abordagens de segurança mais robustas e holísticas, mitigando vulnerabilidades potenciais em todos os âmbitos.

Em suma, nada obstante o avanço normativo no tema, a atuação coordenada entre os órgãos reguladores, o poder legislativo e a iniciativa privada, por exemplo, por meio de mecanismos colaborativos de participação social (e.g., audiências públicas, AIR, consulta públicas, entre outros), é medida essencial para minimizar lacunas e divergências interpretativas, garantir uma maior conformação legal e normativa, reduzir assimetrias e promover uma abordagem mais coesa à proteção de dados pessoais no país.



VEIRANO ADVOGADOS

A Experiência Veirano conta com uma abordagem holística, multidisciplinar e orientada para negócios. A fim de suprir todas as necessidades relacionadas à LGPD, nosso time de Proteção de Dados & Privacidade desenvolveu diversos formatos de projetos, que compreendem diferentes escopos de trabalho para atender demandas específicas de cada um dos nossos clientes:

1. Adequação completa

Com a atuação de uma equipe multidisciplinar, este projeto é destinado aos clientes que possuem como objetivo identificar e avaliar todas as atividades de Tratamento realizadas pela sua empresa e, a partir disso, identificar as vulnerabilidades e estruturar um plano de ação para criação de um programa de privacidade, proteção de dados embasado em pilares jurídico, processuais, de segurança da informação e governança corporativa.

2. *DPO as a service*

Neste modelo, assumimos a função de Encarregado (DPO) em nome do cliente. Para isso, alocamos um profissional para executar as atividades de gestão e monitoramento do programa de proteção de dados e privacidade do cliente.

3. Assessoria em M&A

Criado para assessorar clientes nos processos de auditoria legal de operações de fusão e aquisição, com o propósito de identificar questões de natureza jurídica relevantes (*red-flags*) e mitigar riscos relacionados à proteção e segurança de dados pessoais da empresa-alvo.

4. LGPD Pocket

Uma assessoria “pocket” para a adequação das atividades e/ou dos produtos desenvolvidos pela empresa, independentemente de seu porte ou linha de negócios, com um número reduzido de entregáveis.

5. LGPD on Demand

O LGPD on Demand é direcionado às organizações que desejam contar com uma assessoria multidisciplinar jurídica, de segurança da informação e governança corporativa, com atuação pontual e específica, relacionada a proteção de dados pessoais.

6. LGPD Legal Helpdesk

O Helpdesk foi criado para assessorar clientes em consultas e demandas sobre proteção de dados dentro de um pacote mensal de horas, seja antes, durante ou após o processo de adequação inicial.

7. Task Force para avaliação e comunicação de incidentes de segurança (VA Cybersecurity)

Assessoria jurídica específica e multidisciplinar para aspectos relacionados à suspeita ou ocorrência de um Incidente de Segurança, de acordo com as instruções mais atualizadas da ANPD e demais leis e regulamentos aplicáveis ao tema.

8. Representação em ações administrativas e judiciais envolvendo proteção de dados

Representação de clientes em ações ou potenciais ações administrativas e/ou judiciais em matéria de proteção de dados.

9. Análise de decisões administrativas e judiciais sobre proteção de dados

Monitoramento periódico de decisões proferidas em processos judiciais e administrativos, a fim de apresentar o entendimento das autoridades e os impactos para a empresa ou setor econômico ao cliente de forma resumida.

10. Elaboração e atualização de relatório de impacto à proteção de dados

A ANPD poderá solicitar ao Controlador o Relatório de Impacto à Proteção de Dados Pessoais (“RIPD” ou, em inglês, “DPIA”). Nossa equipe possui expertise no tema, e pode auxiliar com a elaboração e atualização do RIPD.

11. Desenvolvimento de workshops

Elaboração e aplicação de treinamentos sobre os principais conceitos de privacidade e proteção de dados para capacitação de seus colaboradores.

12. Playbook para negociação de contratos comerciais

Elaboração de *playbooks* para negociação e contratos comerciais, para facilitar e agilizar processos internos de equipes comerciais, técnicas e jurídicas.

13. Handbook para resposta aos titulares

Elaboração de materiais para auxiliar as empresas no atendimento tempestivo das solicitações dos titulares, bem como no procedimento a ser seguido pela empresa na resposta ao titular, conforme o modelo de negócio da companhia.

14. Transferência internacional de dados

Ajudamos clientes a entender o contexto da transferência internacional, adequá-la ao fundamento legal aplicável, avaliar requisitos de localização de dados, aditar contratos, elaborar e revisar acordos intragrupo e, de forma geral, responder consultas relacionadas à harmonização da legislação estrangeira com a brasileira.

15. Auditoria de privacidade e proteção de dados

Realizamos auditorias para avaliação do nível de maturidade da companhia, apresentando recomendações para mitigação de risco.

16. Elaboração e revisão de documentos pertinentes ao setor financeiro

Nosso time tem expertise em elaborar políticas de segurança em conformidade com as regulamentações específicas de segurança da informação do Banco Central, além de responder consultas sobre o tema.

17. Elaboração de política de uso de IA

A rápida evolução da IA trouxe inúmeras oportunidades, mas também desafios em relação à ética, privacidade e conformidade. Assim, é imprescindível para o sucesso das empresas ter uma política robusta de uso de sistemas e aplicativos de IA que garanta sua aplicação responsável e eficaz em seus negócios.

Estamos à disposição caso tenha dúvidas ou precise de informações adicionais



ANA CLAUDIA BEPPU
+55 11 2313-5782
ana.beppu@veirano.com.br



ENRICO ROMANIELO
+55 11 2313 5843
enrico.romanielo@veirano.com.br



FÁBIO PEREIRA
+55 11 2313 5906
fabio.pereira@veirano.com.br



GABRIELA ANDRADE GUIMARAES DE OLIVEIRA
+55 21 3824 4637
gabriela.guimaraes@veirano.com.br



PAOLA LORENZETTI
+55 11 99976 8480
paola.lorenzetti@veirano.com.br

Disclaimer: Este material foi atualizado pela última vez em 21 de setembro de 2023 e publicado em 22 de setembro de 2023. Para informações mais atualizadas, entre em contato conosco.