CARTILHA DE PROTEÇÃO DE DADOS PESSOAIS

LTSA advogados

ABEMD

COMUNICADO

A ABEMD, entidade civil fundada por pessoas (físicas e jurídicas) interessadas na aplicação das estratégias e técnicas de Marketing de Dados, discute o tema da Proteção de Dados Pessoais no Brasil de forma intensa há aproximadamente 10 (dez) anos, sempre assessorada de seu consultor jurídico Vitor Morais de Andrade e da equipe de Direito Digital do LTSA advogados.

Estes anos de discussões sobre o tema foram momentos de grande aprendizado para o Setor, inclusive em relação ao nosso relacionamento com as Instituições deste país, tendo a ABEMD participado ativamente do processo legislativo que culminou na LGPD por meio de audiências públicas, reuniões com autoridades, manifestações abertas.

A ABEMD acredita que a LGPD reflete os anseios do setor e a defesa do consumidor, estabelecendo equilíbrio entre a proteção de dados pessoais e a livre circulação de dados.

Diante deste entendimento e com o intuito de demonstrar ao Setor da Comunicação Social os principais pontos de atenção trazidos pela LGPD, bem como o necessário para que as empresas se programem e adequem, a ABEMD em conjunto com o LTSA advogados desenvolveu a presente cartilha sobre proteção de dados pessoais no Brasil e a Lei Federal nº. 13.709/18 (LGPD).

Vitor Morais de Andrade
Assessor Jurídico

Antonio Rosa Neto
Presidente da ABEMD

INTRODUÇÃO

Após mais de 10 anos de debates, finalmente em 2018 foi sancionada a Lei Geral de Proteção de Dados (LGPD – Lei Federal nº. 13.709/2018), que dispõe sobre a proteção de dados pessoais no Brasil. A nova legislação colocou em evidência a necessidade urgente das empresas brasileiras de priorizar a forma correta de coleta e tratamento de dados, em respeito principalmente aos seus titulares.

Os setores de marketing e publicidade digital serão um dos setores mais impactados com as mudanças estabelecidas pela nova lei de proteção de dados. Por tratarem diretamente com gestão de dados pessoais, vendendo serviços como: entrega de análises de preferências e análises de comportamento do consumidor, e principalmente, pela criação de modelos preditivos, tornam-se os setores de maior risco diante da nova legislação.

E apesar da vigência da LGPD ter sido postergada para agosto de 2020, ainda há muito a ser feito. E por isso, quanto antes se iniciarem as mudanças para adequação com a nova legislação, maiores serão as chances de estar de acordo com a lei em tempo.

Para tanto, a presente Cartilha busca de forma simples e objetiva apresentar as principais informações sobre a Lei Geral de Proteção de Dados para que as empresas sejam capazes de avaliar os riscos e necessidades futuras.

PORQUE A PROTEÇÃO DE DADOS É IMPORTANTE?

Na atual sociedade da informação é certo que todas as empresas, independentemente de seu ramo de atuação, tratam dados pessoais, o que consequentemente as submetem à legislação. Isso porque, mesmo que a empresa em questão não trate diretamente de dados como produto principal, é indiscutível que muito provavelmente trata dos dados pessoais de todos seus colaboradores, por exemplo.

Diante disso, tornou-se imprescindível à existência de legislação que determinasse os ditames acerca do uso de dados, que até o momento era feito de modo irrestrito e independente.

Os dados pessoais utilizados pertencem aos seus titulares, e não devem ser utilizados de modo diverso do determinado no momento de seu compartilhamento. Contudo, a ausência de legislação vigente, despertou um mercado de dados descontrolado, deixando a mercê os titulares desses dados.

A utilização de dados pessoais se tornou produto principal da economia digital, e seu uso inconsequente, desrespeita o direito do titular de sua intimidade e principalmente privacidade.

A regulamentação sobre proteção de dados, além de garantir a proteção dos dados pessoais, também procura garantir uma mudança na forma como as empresas abordam gestão de dados, e consequentemente, acaba por criar um mercado de dados de maior qualidade e maior valor agregado.

Sem deixar de mencionar que para as empresas que conseguirem se adaptar antes, haverá uma grande vantagem econômica diante daquelas que ainda não começaram o processo de adaptação, visto que já poderão oferecer seus serviços e produtos de forma adequada.

Uma maior regulamentação e fiscalização geram um maior compromisso e confiabilidade ao mercado, possibilitando uma maior confiança de clientes e consumidores pela transparência no uso de seus dados.

PORQUE A PROTEÇÃO DE DADOS É IMPORTANTE?

Sobre o assunto, segue de forma clara os objetivos e vantagens resultantes da LGPD:

Objetivos	Vantagens
Garantir maior transparência ao uso de dados pessoais	Possibilita que as empresas façam inovações responsáveis
Garantir a inviolabilidade da intimidade, da honra e da imagem	Cria um mercado baseado na confiança de clientes e consumidores
Garantir o direito do consumidor	De certa forma, garante que as empresas estejam aptas para a economia digital.
Proporcionar mais confiabilidade com a sociedade	Possibilidade de melhorar a relação com países que já têm leis de proteção de dados
Garantir segurança jurídica em face de uma sociedade digital	Gera maior valor agregado aos dados coletados de forma regular e com origem definida.
Atribuir maior rigor ao tratar dados de seus titulares e assim mudar a forma como as empresas abordam gestão de dados	Aqueles que se adaptarem mais cedo contarão com um diferencial de mercado, podendo oferecer seus produtos e serviços com a vantagem de já estarem de acordo com a legislação.

CONCEITOS RELEVANTES

O QUE SÃO DADOS PESSOAIS? E DADOS PESSOAIS SENSÍVEIS?

Conforme estabelece a Lei Geral de Proteção de Dados (LGPD) e a legislação europeia (*General Data Protection Regulation* - GDPR), dados pessoais são informações relacionadas à pessoa natural, que possibilitam sua identificação direta ou indiretamente (art.5º, I, LGPD). Exemplos de dados pessoais são data de nascimento, CPF, RG, profissão, entre outros.

Dentro dos dados pessoais, existem dados pessoais denominados sensíveis, que consistem basicamente de dados relacionados à pessoa natural identificada ou identificável, por meio dos quais é possível discriminar um indivíduo. Sendo então, considerado dado sensível todo dado pessoal que verse sobre: (i) origem racial ou étnica; (ii) convicção religiosa; (iii) opinião política; (iv) filiação a sindicato ou a organização de caráter religioso, filosófico ou político; (v) dado referente à saúde ou à vida sexual; (vi) dado genético ou biométrico, quando vinculado a uma pessoa natural (art.5º, II, LGPD).

NO QUE CONSISTE O TRATAMENTO DE DADOS?

A LGPD apresentou em seu escopo o conceito de tratamento de dados pessoais, enumerando um rol exemplificativo das ações que se enquadram nessa categoria. Conceituando o tratamento de dados como toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (art.5º, inciso X, LGPD).

COMO IDENTIFICAR OS AGENTES DE TRATAMENTO DE DADOS? E QUAL A RELEVÂNCIA DESSA DIFERENCIAÇÃO?

Conforme determina a LGPD, agentes de tratamento é gênero dos quais são espécies o controlador e o operador (art. 5°, IX, LGPD). Sendo o controlador de dados aquele responsável por tomar decisões acerca do tratamento de dados, enquanto que o operador de dados, seguindo as instruções do controlador, operacionaliza o tratamento dos dados pessoais.

A identificação dos agentes é parâmetro fundamental no caso de dano causado a outrem em razão do exercício de atividade de tratamento de dados pessoais, posto que a violação a legislação de proteção de dados gera obrigação de reparação. Nesse caso, a identificação se torna essencial na apuração de corresponsabilidade no caso de indenização (art. 42°, §1°, LGPD).

Além disso, a identificação dos agentes de tratamento é fundamental para cobrança do registro das operações de tratamento de dados pessoais realizados, principalmente, nos casos em que a coleta está fundada somente no legítimo interesse.

Conforme a Lei Geral de Proteção de Dados o relatório deverá conter, no mínimo: (i) a descrição dos tipos de dados coletados; (ii) a metodologia utilizada para a realização da coleta e para a garantia da segurança da informação; e (iii) a análise do controlador com relação as medidas (art. 38, parágrafo único, LGPD), e poderá ser solicitado pela Autoridade Nacional a qualquer tempo.

PRIVACY BY DESIGN E PRIVACY BY DEFAULT

O *privacy by design* representa o emprego de mecanismo de privacidade em todo o ciclo do dado utilizado. É incorporar a privacidade ao desenho do produto ou serviço, protegendo todo o ciclo do dado e concedendo-lhe proteção de ponta a ponta.

Enquanto o *privacy by default* se baseia em entender a privacidade como modelo de conduta, minimizando processamento de dados pessoais, utilizando-se de técnicas como pseudononimização e criptografia. Ou seja, buscar estabelecer como padrão a configuração que concede a maior privacidade ao titular dos dados.

Tais modelos refletem a forma como os agentes de tratamentos devem tratar os dados pessoais, de forma a adotar durante todo o ciclo dos dados medidas de segurança capazes de efetivamente protege-los.

PRINCÍPIOS DA PROTEÇÃO DE DADOS NO TRATAMENTO DE DADOS

A LGDP enumera os princípios norteadores para manuseio e tratamento dos dados, totalizando assim, uma lista de 10 princípios (art.6°, LGPD), sendo eles:

• **Finalidade**: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

• **Adequação**: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

• **Necessidade**: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

• **Livre acesso**: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

• **Qualidade dos dados**: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

• **Transparência**: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

• **Segurança**: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

• **Prevenção**: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

• **Não discriminação**: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

• **Responsabilização e prestação de contas**: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

E QUAIS SÃO AS BASES LEGAIS PARA O TRATAMENTO DE DADOS?

As empresas devem se organizar de forma que o tratamento de dados para marketing ocorra de acordo com o disposto na Lei Geral de Proteção de Dados e demais legislações específicas relacionadas ao tema. Faz-se necessário compreender que os dados coletados pertencem ao indivíduo, ao qual dizem respeito, sendo certo que a coleta ou qualquer outro tipo de tratamento estão condicionados a certos requisitos.

A coleta e tratamento de dados devem sempre ser realizados de forma específica, explícita e para propósitos legítimos, sendo estritamente proibida a utilização dos dados coletados para finalidade diversa da informada no momento da coleta.

Desta forma, devem as empresas se atentar aos requisitos de coleta e uso de dados pessoais, que sempre deverão se basear em uma das seguintes hipóteses (art. 7º, LGPD):

• consentimento (escrito ou por meio que demonstre a vontade do titular);

• cumprimento de obrigação legal;

• necessidade para execução contratual;

• exercício regular de direitos em processo judicial, administrativo ou arbitral;

• proteção à vida ou incolumidade física do titular ou de terceiro;

• para a tutela da saúde;

• para atender a legítimo interesse do controlador (quem exerce poder de decisão sobre o tratamento dos dados) ou terceiro;

• para a proteção de crédito; e,

• em razão da publicidade dada aos dados por seu titular ou do acesso público irrestrito a este, desde que observados a finalidade com que o dado fora disponibilizado, a boa-fé e não fira direitos e garantias fundamentais.

E NO CASO DA OCORRÊNCIA DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO?

No caso de qualquer incidente envolvendo quebra de segurança da informação e consequente vazamento de dados pelas áreas de negócios, parceiros, clientes, colaboradores e terceiros, que possa acarretar risco ou dano relevante aos titulares dos dados, deve a empresa realizar comunicação em tempo razoável, conforme será definido pela Autoridade Nacional de Proteção de Dados.

A Comunicação deverá descrever: (i) a natureza da violação de dados (indicando categorias e número aproximado de titulares afetados); (ii) a descrição das prováveis consequências; (iii) descrever as medidas tomadas para atenuar a violação ou suas consequências (art. 48, §1°, LGPD).

A Autoridade Nacional de Proteção de Dados verificará a gravidade do incidente, e caso necessário para proteção dos direitos dos titulares, poderá determinar ao controlador a tomada de providências como: (i) ampla divulgação do fato em meios de comunicação; e (ii) medidas para reverter ou mitigar os efeitos do incidente.

QUEM É RESPONSÁVEL PELO MONITORAMENTO DO CUMPRIMENTO DA L.13709/18?

Inicialmente, a LGPD fora publicada em 15 de agosto de 2018 com vetos aos artigos referentes a criação da Autoridade Nacional de Proteção de Dados (artigos 55 a 59 da LGPD), o que resultou em um ambiente de insegurança quanto a aplicação da lei. Contudo, no dia 9 de julho de 2019, quase onze meses após a publicação da LGPD, foi publicada a Lei 13.853, que alterou os dispositivos da Lei, e criou a Autoridade Nacional de Proteção de Dados (ANPD).

Tais modificações determinaram a instituição da ANPD como órgão da administração pública federal indireta vinculada a Presidência da República. Com a função de (art. 55-J, LGPD):

(I) zelar pela proteção dos dados pessoais, nos termos da legislação;

(II) zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos da LGPD;

(III) elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;

(IV) fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;

(V) apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação;

(VI) promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;

(VII) promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;

(VIII) estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis;

(IX) promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;

QUEM É RESPONSÁVEL PELO MONITORAMENTO DO CUMPRIMENTO DA L.13709/18?

(X) dispor sobre as formas de publicidade das operações de tratamento de dados pessoais;

(XI) solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar;

(XII) elaborar relatórios de gestão anuais acerca de suas atividades;

(XIII) editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD;

(XIV) ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento;

(XV) arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas;

(XVI) realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público;

(XVII) celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942;

(XVIII) editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei;

(XIX) garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso);

QUEM É RESPONSÁVEL PELO MONITORAMENTO DO CUMPRIMENTO DA L.13709/18?

(XX) deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos;

(XXI) comunicar às autoridades competentes as infrações penais das quais tiver conhecimento;

(XXII) comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal;

(XXIII) articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e

(XXIV) implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei.

Concluindo-se, assim, é a ANPD responsável por fiscalizar, monitorar e aplicar as sanções cabíveis quando do descumprimento da LGPD, e pelas demais disposições funcionais acima elencadas.

QUAIS AS CONSEQUENCIAS PARA QUEM NÃO ESTIVER PREPARADO?

A LGPD enumera as possíveis sanções a serem aplicadas em razão de infrações cometidas (art. 52, LGPD):

• **Advertência**: com indicação de prazo pela Autoridade Nacional de Proteção de Dados para adoção de medidas corretivas;

• **Multa**: que será aplicada pela Autoridade Nacional de Proteção de Dados de acordo com a especificidade de cada caso, podendo aplicar multa simples ou diária de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, limitada no total a R$ 50.000.000,00 por infração.

• **Publicização**: no caso de incidentes de segurança da informação, a Autoridade Nacional de Proteção de Dados poderá determinar a publicização da infração após sua apuração e confirmação de ocorrência.

• **Bloqueio dos dados**: a que se refere a infração até a sua regularização.

• **Eliminação dos dados**: a que se refere a infração.

Ressalta-se que as sanções somente serão aplicadas após procedimento administrativo que possibilite a oportunidade de ampla defesa, de acordo com as peculiaridades do caso concreto (art. 52, §1°, L. 13709/18).

COMO AS EMPRESAS DEVEM SE ADEQUAR?

As empresas têm até agosto de 2020 para se adaptarem até a entrada em vigor da LGPD, e apesar de parecer muito tempo, pode não ser o suficiente para alguns a depender de sua maturidade no assunto.

Portanto, quanto mais cedo as empresas começarem a se preparar, maiores as chances de conseguirem se adaptar a LGPD a tempo. Nesse sentido, seguem algumas sugestões de ações para adequação:

• Estabelecer uma política corporativa de privacidade: com a função de criar uma cultura empresarial baseada na proteção de dados pessoais, cultura esta que deverá ser aderida pelos funcionários, parceiros e clientes.

• Elaborar cláusulas contratuais para regulamentar tratamento de dados que: vincule o subcontratante (operador/controlador) ao responsável (controlador), estabeleça o objeto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, as obrigações e direitos do responsável pelo tratamento.

• Ater-se, no tratamento, à finalidade determinada com a qual o dado fora compartilhado pelo titular (art.6º, LGPD).

• Segurança: utilização de medidas técnicas aptas a proteger os dados de acessos não autorizados, situações acidentais ou ilícitas (art.6º e 46, LGPD).

• Prestação de contas: demonstração de medidas eficazes e capazes de comprovar a observância e cumprimento das normas de proteção de dados pessoais (art.6º, LGPD).

• Somente realizar tratamento de dados pessoais frente a uma das hipóteses/bases legais (art.7º, LGPD).

• Caso venha a realizar o tratamento de dados pessoais sensíveis, somente o fazê-lo, sob pena de descumprimento da Lei, mediante: (i) consentimento específico e em destaque; (ii) obrigação legal; (iii) exercício regular de um direito; (iv) proteção à vida ou incolumidade física do titular ou de terceiro; (v) para a tutela da saúde; (vi) garantia de prevenção à fraude e segurança do titular. Não tratar dados sensíveis referente à saúde para obtenção de vantagem econômica, exceto nas hipóteses enumeradas (art.11, LGPD).

COMO AS EMPRESAS DEVEM SE ADEQUAR?

• Não realização de tratamento para fins discriminatórios ilícitos ou abusivos (art.6º LGPD);

• Exigir para o tratamento de dados de crianças diante do consentimento específico e em destaque de pelo menos um dos pais ou responsável (art.14, §1º, LGPD).

• Manter registros das operações de tratamento de dados pessoais que realizar (art.37, caput, LGPD).

• Formular (regras de boas práticas e governança sobre proteção de dados pessoais (art.50, LGPD)

• Nomear um encarregado pelo tratamento de dados pessoais (art.41, LGPD), caso seja classificado como "controlador", atentando-se as normas emitidas pela ANPD, posto que, conforme definição do artigo 5, inciso VIII, poderá ser necessário a indicação de encarregado para empresa classificada como "operador".

• Elaborar relatório de impacto à proteção de dados pessoais, referente às suas operações de tratamento (art.38, LGPD).

• Ser capaz de conceder ao titular o direito de acesso, retificação, cancelamento e portabilidade dos dados pessoais, quando se comportar como controlador dos dados, disponibilizando um canal próprio para isso. Exigir que eventuais retificações/cancelamento dos dados sejam replicados ao longo da cadeia de tratamento.

• Escolher parceiros com o mesmo nível de proteção de dados pessoais.

• Seguir um Programa *Compliance* de Adequação a Lei Geral de Proteção de Dados Pessoais, bem como estas e demais orientações a serem emitidas pela ABEMD.

FICHA TÉCNICA

ELABORAÇÃO

Vitor Morais de Andrade

Assessor da ABEMD, é sócio no escritório LTSA Advogados. Graduado em Direito pela Pontifícia Universidade Católica de São Paulo (PUC/SP), é Mestre e Doutor em Direito das Relações Sociais pela Pontifícia Universidade Católica de São Paulo (PUC/SP). Professor e Coordenador do Curso de Graduação da Faculdade de Direito da Pontifícia Universidade Católica de São Paulo (PUC/SP). Possui pós-graduação em Economia pela FGV-SP (PEC – Programa de Educação Continuada) e *Negotiation and Leadership na Harvard Law School*. Atuou como Coordenador Geral do Departamento Nacional de Proteção e Defesa do Consumidor do Ministério da Justiça – DPDC/SDE/MJ, é membro efetivo da Comissão de Direito das Relações de Consumo da OAB/SP e atuou como Presidente da Associação Brasileira de Relações Empresa-Cliente, ABRAREC. É Árbitro da Câmara de Mediação e Arbitragem da FIESP / CIESP, Professor da Faculdade de Direito da Pontifícia Universidade Católica de São Paulo (PUC/SP) para cursos de graduação e pós-graduação lato sensu e Conselheiro no Conselho Nacional de Autorregulação Publicitária – CONAR.

Área de Direito Digital e Proteção de Dados
Contato: direitodigital@ltsa.com.br