Apresentação

O aperfeiçoamento das questões que envolvem os dados pessoais nas últimas décadas reflete a expressão de sua exponencial relevância tal qual direito fundamental autônomo para a tutela da pessoa humana. Desse modo, a proteção de dados passa a contribuir para a constitucionalização da pessoa, fator que pode ser considerado um enorme alcance jurídico. Percebe-se que a proteção de dados se encontra em uma verdadeira reinvenção, não apenas por ser considerada direito fundamental, mas por ter se tornado ferramenta essencial para o livre desenvolvimento da personalidade.

Assim, com o desenvolvimento tecnológico acelerado e a solidificação de espaços virtuais públicos, a gerência da informação tornou-se ferramenta essencial do indivíduo. Consequentemente, não se faz possível a cogitação quanto à integral proteção à liberdade, à privacidade e ao desenvolvimento da pessoa natural sem que, da mesma forma, lhe sejam garantidos a defesa e o controle de seus dados pessoais.

Dessa forma, não apenas no Brasil, mas em uma escala global, a administração dos dados passou a ser regulamentada, com especial atenção à legislação pátria, por meio da Lei no 13.709/2018, mais conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), a qual pretende proteger o usuário-cidadão em todos os aspectos de sua autonomia pública e privada, valorizando e preservando a autodeterminação informativa e sua capacidade decisória.

Nesta Unidade de Aprendizagem, você irá conhecer quais são os fundamentos teóricos e históricos da proteção de dados. Irá compreender os conceitos, princípios e institutos que balizam a LGPD e, ainda, aprender sobre o uso desta nas áreas da educação, saúde e relações trabalhistas.

Bons estudos.

Ao final desta Unidade de Aprendizagem, você deve apresentar os seguintes aprendizados:

- Apresentar os fundamentos teóricos e históricos da proteção de dados pessoais.
- Analisar os conceitos, princípios e institutos da Lei Geral de Proteção de Dados (LGPD).
- Definir o uso da LGPD nas áreas da educação, saúde e relações trabalhistas.

Infográfico

Como inovação jurídica, a LGPD trouxe a especial tratativa e aspectos de transparência na forma como empresas, incluindo aquelas voltadas à educação, devem coletar, armazenar e compartilhar a informação das pessoas. Uma especial vantagem diz respeito a maior segurança jurídica ofertada para pessoas físicas e jurídicas, naquilo que está relacionado às informações privadas. Baseada e impulsionada pela General Data Protection Regulation (GDPR) da União Europeia, a legislação brasileira reúne conceitos e diretrizes no tratamento de dados pessoais, indicando, de maneira criteriosa, um roteiro sobre o que as empresas devem fazer para que o tratamento do dado pessoal seja lícito e não passível que irregularidades, as quais estão sujeitas a autuações e aplicação de multas.

Entre tantas outras, a área da educação foi afetada diretamente pela entrada em vigor da LGPD e, com isso, aspectos básicos passaram a ser passíveis de revisão e adequação pelas instituições de ensino. Nesse sentido, questões vinculadas ao marketing institucional, à política de *data retention* e à definição do que são dados essenciais para a prestação do serviço de educação e quais são meramente suplementares passaram a ser fundamentais para a adequação das instituições de ensino à legislação de proteção de dados brasileira.

Neste Infográfico, você verá alguns dos aspectos importantes da adequação do cotidiano das instituições de ensino à LGPD, em aspectos relativos ao tratamento de dados pessoais na educação e à conformação à nova lei sobre a temática.

LGPD NA EDUCAÇÃO: MUDANÇAS NO COTIDIANO DAS INSTITUIÇÕES DE ENSINO

A LGPD foi sancionada pelo então presidente Michel Temer, após inúmeros debates e ponderações. Com a nova lei, o Brasil passa a compor um grupo de 120 países que têm lei específica para a proteção de dados pessoais, baseando-se na GDPR – regulamentação europeia sobre privacidade e proteção de dados pessoais –, o que passou a modificar inúmeras áreas do conhecimento, entre elas a educação, conforme exposto a seguir:

O que diz a LGPD?

Trata-se de instrumento que trabalha com a **ampliação do aumento da proteção e privacidade no tratamento de informações pessoais**.

Assim, órgãos responsáveis passam a exercer maior fiscalização e controle das empresas, com destaque para as organizações que trabalham direta e frequentemente com dados de pessoas físicas, as quais passam a ser diretamente atingidas pelas diretrizes na Lei nº 13.709/2018, o que, por conseguinte, requer modificações e adaptações de processos.

Tratamento de dados na educação

Consiste em tratamento de dados qualquer operação que seja concebida por meio de um dado pessoal, logo utilização, reprodução e armazenamento são alguns exemplos de tratamentos de dados.

Com **o advento da LGPD**, as instituições de ensino devem ser específicas, em todas as ocasiões, **sobre a verdadeira necessidade da requisição de determinado** dado – o que se denomina de **motivação**.

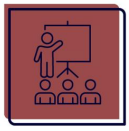
LGPD na educação: o que é alterado?

Com a lei nova, as instituições de ensino precisam reanalisar seus processos de coleta e uso de dados de alunos. Logo, a repercussão da LGPD na educação é refletida tanto na **captação de alunos** – processos de atração e geração de *leads*, como na **gestão da permanência** – por meio de ações preventivas à evasão.

Como a LGPD afeta o cotidiano das instituições de ensino?

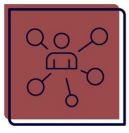
Altera a forma de desenvolvimento de marketing de conteúdo educacional, com a necessidade do **consentimento explícito do *lead***, ou seja, o aluno deve estar consciente e conceder ativamente o **uso e tratamento de seus dados**, sendo necessário que o usuário esteja ciente da forma **como as informações poderão ser utilizadas**.

Objetivando diminuir os impactos da LGPD na educação, faz-se necessário o investimento na **capacitação dos funcionários das instituições de ensino** que, apenas por meio de diretrizes claras, obterão êxito na implantação das novas práticas.



As instituições de ensino precisam investir em **ações preventivas e planos de emergência**, uma vez que a lei prevê multa de até 2% do faturamento líquido da pessoa jurídica de direito privado no total de até 50 milhões por infrações vinculadas com o vazamento de dados pessoais dos usuários. Ademais, infrações dessa natureza afetam diretamente no capital reputacional da empresa no mercado, ou seja, como a instituição de ensino passa a ser vista por futuros alunos e professores.

Investimento das instituições de ensino em CRM (*Customer Relationship Management*) para educação minimiza os impactos da LGPD, uma vez que fortifica a garantia para a segurança e tratamento dos dados dos usuários.



Com o direcionamento de ações para a adequação à LGPD, as instituições de ensino ficam protegidas de sanções pelo descumprimento das novas regras e, além disso, ganham melhor posicionamento no mercado, pois seus alunos, professores e operadores passam a ter seus dados protegidos pelos mecanismos motivadores ao cumprimento com a LGPD.

Aponte a câmera para o código e acesse o link do conteúdo ou clique no código para acessar.

Conteúdo do Livro

O desenvolvimento social passou por enormes alterações nos últimos anos. Desde a forma como a comunicação passou a ser desenvolvida, até os mais delicados modos de estabelecimento de relações internacionais mudaram de lentes e passaram a ganhar muitas informações com o advento do crescimento do acesso à internet. Essa alteração no comportamento humano de estabelecer relações sociais também foi motivo de alteração na forma como os dados pessoais passaram a ser cada vez mais valiosos.

Assim, em uma escalada global, o fornecimento de informações passou a ser corriqueiro no dia a dia das pessoas para os mais diferentes ramos: seja para a troca de mensagens, a realização de uma transação bancária, a forma de aprendizagem no ambiente virtual e tantas outras centenas de atividades.

Com isso, a gestão dos dados passou a ser observada de maneira mais atenta por parte do poder público, preocupado com a garantia dos direitos fundamentais e da Carta Magna, além dos preceitos que já traziam resquícios quanto à proteção de dados em instrumentos infraconstitucionais.

Os escândalos de vazamento de dados, impulsionaram a criação de regulações específicas à proteção de dados, com especial destaque para a GDPR na União Europeia e, evidentemente, a LGPD no Brasil, a qual passou a ser o instrumento de guarida do tratamento dos dados pessoais no âmbito nacional, objetivando proteger a privacidade, a liberdade e o desenvolvimento da pessoa natural.

No capítulo Proteção de dados pessoais, base teórica desta Unidade de Aprendizagem, você irá entender quais são os fundamentos teóricos e históricos da proteção de dados, irá estudar os conceitos, os princípios e os institutos da LGPD e conhecerá o uso da LGPD nas áreas da educação, saúde e relações trabalhistas.

Boa leitura.

DIREITO DIGITAL

SOLUÇÕES EDUCACIONAIS INTEGRADAS

Proteção de dados pessoais

Karoline Freire

OBJETIVOS DE APRENDIZAGEM

- Apresentar os fundamentos teóricos e históricos da proteção de dados pessoais
- Analisar conceitos, princípios e institutos da Lei Geral de Proteção de Dados (LGPD).
- Definir o uso da LGPD nas áreas de educação, saúde e relações trabalhistas

Introdução

O aperfeiçoamento das discussões relativas aos dados pessoais nas últimas décadas representa a ênfase de sua relevância como direito fundamental autônomo para a tutela dos cidadãos. Com a rapidez dos avanços tecnológicos e a difusão em larga escala do acesso ao ambiente virtual, o manejo das informações sobre si próprio se tornou expressão essencial do indivíduo. Logo, torna-se impossível cogitar a integral proteção da liberdade, da privacidade e do desenvolvimento da pessoa natural sem que lhe seja garantida a eficiente defesa e o controle dos próprios dados, ou seja, a expressão da autodeterminação informativa.

Diante dos requerimentos sociais de uma nova instituição legislativa especializada na proteção dados, nasceu a denominada Lei Geral de Proteção de Dados (LGPD), a Lei nº 13.709 de 2018 (BRASIL, [2019]), que passou a dispor sobre o tratamento de dados pessoais, inclusive no ciberespaço, por pessoa natural ou jurídica, de direito público ou privado, com o intuito de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, conforme dispõe o artigo inaugural do documento

legal. Assim, os mais diferentes âmbitos sociais, como saúde, educação e relações de trabalho, passam a ter a necessidade de se adequar à LGPD, para um melhor desenvolvimento da sociedade e da proteção à dignidade da pessoa humana e dos preceitos trazidos na Constituição de 1988 (BRASIL, [2016]).

Neste capítulo, você vai conhecer os fundamentos teóricos e históricos da proteção de dados pessoais. Além disso, vai ver conceitos, princípios e institutos da LGPD, com destaque ao tratamento de dados e ao consentimento. Por fim, vai estudar a LGPD nas áreas da educação, saúde e relações trabalhistas.

Proteção de dados pessoais: fundamentos teóricos e históricos

Inaugurando a redação da LGPD, o artigo 1º define o alcance da proteção de dados pessoais, os quais estão vinculados tanto para o ambiente físico quanto para o digital, certificando como sujeito de direitos unicamente a pessoa natural identificada ou identificável (BRASIL, [2019]). O documento legal indica que o objetivo requerido é a proteção dos direitos fundamentais da liberdade e privacidade, além do livre desenvolvimento da pessoa natural. Finalmente, dirige-se para pessoa física ou jurídica, de direito público ou privado, que trabalhe com dados da pessoa natural (BRASIL, [2019]).

O desenvolvimento de regulações específicas à proteção de dados também ganhou, ao longo dos anos, respaldo teórico, com atenção para preceitos advindos da Carta Maior (BRASIL, [2016]), entre eles a privacidade. O descontrole e a incerteza sobre aquele que tem o direito ao acesso aos dados pessoais perpassa o poder de escolha que delimita e define a esfera pessoal de cada ser humano. A necessidade de tutela jurídica aos que confiam seus dados pessoais às entidades públicas ou privadas se tornou evidente à medida que esses dados têm valor econômico e são usados para fins comerciais (PEZZI, 2007).

Nesse contexto, antes da edição da lei de proteção de dados, havia um debate teórico relacionado aos limites da privacidade, uma vez que os bancos de dados armazenavam — e continuam armazenando — milhões de dados pessoais, o que, na verificação da doutrina, parecia ultrapassar os direitos das pessoas em relação à gestão de seus dados. Assim, os bancos de dados se tornaram um instrumento perfeito para dilacerar os limites da privacidade. Os bancos de dados permitiam que fossem criados perfis específicos de acordo com os interesses dos titulares dos dados pessoais, e o acesso a esses bancos tomou uma dimensão ainda mais expressiva pela facilidade de transmissão

e circulação de dados. Assim, diante das relações de consumo, a criação de perfis era perfeita para a fácil e rápida transmissão de dados por meio dessas plataformas de informações pessoais. Um curso de pós-graduação, por exemplo, poderia utilizar um banco de dados de uma editora de livros especializada no segmento do curso para promover as atividades de ensino. Uma empresa de seguro de saúde poderia utilizar o banco de dados de uma loja esportiva para identificar as pessoas que, potencialmente, precisariam de serviços médicos. Uma financeira, apropriando-se de um banco de dados de uma loja de departamentos, poderia oferecer cartões de crédito a quem lhe interessasse o histórico de quitação de pagamentos para concessão da vantagem creditícia (PEZZI, 2007).

> A proporção dos reflexos possíveis com cruzamentos [de dados] se dimensiona de tal forma quando órgãos do próprio Estado tomam iniciativas para disponibilizar informações pessoais de seus cidadãos. Os jornais passam a estampar o debate sobre a possibilidade de empresas terceirizadas administrarem e comercializarem o cadastro de segurança pública do Estado de São Paulo, em troca da modernização do banco de dados. [Permitia-se ainda que] os planos de saúde [acessassem] dados sigilosos do paciente. Mesmo sendo criada para nortear o intercâmbio de dados entre os planos e os prestadores de serviço, melhorar a qualidade de gestação e coletar informações epidemiológicas necessárias para o planejamento de políticas de saúde, a medida [chocava-se] com o sigilo médico-paciente e [fornecia] um manancial de informações para o setor privado das seguradoras de saúde, [que eram capazes] de restringir [o] acesso a possíveis segurados (PEZZI, 2007, p. 11–12).

Logo, as relações de consumo, que já colocam o consumidor como figura vulnerável, passaram a ficar ainda mais instáveis por força do impacto da utilização dos bancos de dados e cadastros de consumidores sem que existisse qualquer regulamentação com embasamento específico para legislar a respeito da proteção de dados.

Foi apenas com o advento da publicação da LGPD que uma lacuna no ordenamento jurídico pátrio foi preenchida, no sentido da proteção de dados pessoais, mas normas anteriores foram precursoras desse propósito. O reconhecimento da proteção de dados como direito autônomo e fundamental advém de considerações dos riscos que o tratamento automatizado traz para a proteção da personalidade em relação às garantias constitucionais de igualdade, liberdade e dignidade da pessoa humana, com destaque, ainda, para a proteção da intimidade e da vida privada. A proteção de dados pessoais no ordenamento jurídico brasileiro, embora hoje desfrute de legislação específica, ganhou respaldo em outros documentos legais (DONEDA, 2011). A Constituição Brasileira contempla a questão da informação por meio das

garantias à liberdade de expressão e do direito à informação, além de fundamentar a proteção da personalidade e o direito à privacidade (BRASIL, [2016]).

Além disso, o Código de Defesa do Consumidor (CDC) de 1990, documento legal que traz, em sua Seção VI, os Bancos de Dados e Cadastros dos Consumidores, garante o direito às informações existentes em relação ao consumidor (BRASIL, 1990). Nesse documento legal, destaca-se o conteúdo do artigo 43, o qual estabelece uma série de direitos e garantias para o consumidor em relação às suas informações pessoais presentes em bancos de dados e cadastros, "[...] implementando uma sistemática baseada nos *fair information principles* à matéria de concessão de crédito e possibilitando que parte da doutrina verifique neste texto legal o marco normativo dos princípios de proteção de dados pessoais no direito brasileiro" (DONEDA, 2011, p. 103). Assim:

> [Parecia] existir no direito brasileiro, de forma generalizada, uma consciência de que seria possível tratar de forma satisfatória os problemas relacionados às informações pessoais em bancos de dados a partir de uma série de categorizações, geralmente generalistas e [...] abstratas: sobre o caráter rigidamente público ou particular de uma espécie de informação; a respeito da característica sigilosa ou não de determinada comunicação, e assim por diante. Enfim: com um sistema baseado em etiquetas, permissões ou proibições para o uso de informações específicas, sem considerar os riscos objetivos potencializados pelo tratamento informatizado das informações pessoais (DONEDA, 2011, p. 104).

Outro documento jurídico especialmente importante à proteção de dados no Brasil é o Marco Civil da Internet, Lei nº 12.965 de 2014 (BRASIL, 2014), o qual assegura aos usuários da rede mundial de computadores a inviolabilidade da intimidade e da vida privada, com destaque para o artigo 7º, incisos I a XIII, que tratam sobre direitos e garantias dos usuários, assegurando o direito às informações de forma clara e completa sobre coleta, uso, armazenamento, tratamento e proteção de dados pessoais. Além disso, o artigo 7º informa o direito do usuário ao consentimento expresso sobre coleta, uso, armazenamento, tratamento e proteção de dados pessoais e a garantia da exclusão definitiva dos dados pessoais fornecidos a determinada aplicação de internet, a requerimento do usuário, ao término das relações entre as partes (BRASIL, 2014).

Assim, é possível perceber que, anteriormente à edição e publicação da LGPD, outros documentos legais já dissertavam, ainda que de forma discreta, sobre a necessidade da proteção de dados. Eles foram impulsionados, por exemplo, pelas revelações sobre as iniciativas de espionagem antiéticas e ilegais do governo norte-americano, como é o caso do Marco Civil da Internet (CARVALHO; OLIVEIRA, 2019).

Porém, essas iniciativas não surgiram apenas de uma preocupação do legislador brasileiro em garantir efetivas responsabilidades e sanções para entidades públicas e privadas quanto ao cuidado com o tratamento de dados. Diversos países no mundo foram impulsionados a criar legislações específicas em matéria de proteção de dados, pois escândalos de vazamento de dados passaram a influenciar processos democráticos importantes, como as eleições presidenciais estadunidenses de 2016 e o plebiscito sobre a saída do Reino Unido da União Europeia (BREXIT), também em 2016.

Um acontecimento notório e de grande repercussão foi o caso envolvendo a empresa Cambridge Analytica, sob a qual se especulava a relação de vendas e o uso indevido de dados na campanha eleitoral de Donald Trump em 2016. O caso veio a público pela primeira vez em dezembro de 2015 e chegou até a corte americana no início de 2018. A rede social Facebook foi responsabilizada pelo caso e penalizada ao pagamento de 5 bilhões de dólares (BISSO *et al*., 2020).

Outros exemplos práticos do vazamento de dados que foram importantes à articulação de autoridades em diversas partes do mundo para tratar os dados pessoais ocorreu com a companhia hoteleira Marriott, que foi multada em 100 milhões de libras esterlinas pelo vazamento de 339 milhões de dados de clientes. Entre esses dados, havia números de cartões de crédito e dados de passaporte. A falha foi decorrente de um sistema adotado pela empresa após a compra de outra rede de hotéis, a Starwood, que já havia sido notificada sobre problemas de segurança em seus sistemas em 2014. Outro caso ocorreu com a companhia aérea British Airways, vítima de um ataque de *hackers*, que afetou mais de 500 mil clientes em 2018. Os dados roubados incluíam o histórico de compra de passagens, informações de pagamentos e informações pessoais de seus usuários, como nome e endereço. A empresa foi responsabilizada ao pagamento de 183 milhões de libras esterlinas pelo acontecimento (BISSO *et al*., 2020).

O indiscriminado vazamento e compartilhamento de dados de forma ilegal em inúmeros casos passou a gerar impactos socioeconômicos expressivos. Segundo informações publicadas em 2018, o custo envolvendo o vazamento de dados, somente nos Estados Unidos, somou 654 bilhões de dólares e expôs 2,4 bilhões de dados de usuários (BISSO *et al*., 2020).

Diante desse cenário, governos passaram a tomar medidas para que empresas aumentassem os investimentos com a segurança dos dados dos usuários. A União Europeia criou, em 2016, uma nova regulamentação para proteção de dados pessoais: a General Data Protection Regulation 2016/679 (GDPR) (UNIÃO EUROPEIA, 2016). Tal instrumento legal foi um importante marco para proteção e privacidade de dados dos cidadãos da União Europeia e do

Espaço Econômico Europeu. Por meio dele, a proteção de dados pessoais passou a ser tratada como direito fundamental (BISSO *et al*., 2020).

Os Estados Unidos, por outro lado, embora inúmeras sanções sejam impostas e notadamente difundidas em relação à proteção de dados, carece de uma legislação federal que regule a matéria de forma específica. Contudo, diferente do que acontece na União Europeia com a GDPR e no Brasil com a LGPD, as leis de segurança e privacidade de dados nos Estados Unidos são específicas, regulamentando, por exemplo, o uso de determinados tipos de dados no setor de saúde, finanças e telecomunicações. Assim, objetivando tratar sobre matérias não legisladas no nível federal, algumas regulações específicas para proteção de dados estaduais são expressivamente importantes, como é o caso do estado da Califórnia, onde a matéria é regulada por meio da California Consumer Privacy Act (CCPA), e do estado de Nova York, com a New York Stop Hacks and Improve Eletronic Data Security Act (NY SHIELD) (BISSO *et al*., 2020).

A legislação sobre proteção de dados brasileira foi notadamente inspirada no regulamento da União Europeia, a GDPR, que entrou em vigor em 2018 e trouxe importantes impactos para empresas e consumidores. Com isso, o Brasil, com o advento da LGPD, que entrou em vigor em 18 de setembro de 2020, passou a compor um grupo de países que contam com legislação específica para a proteção de dados de seus cidadãos. Assim, diante dos atuais casos de uso indevido, comercialização e vazamento de dados, as novas regras passaram a garantir a privacidade dos titulares dos dados pessoais, além de passar a evitar entraves comerciais com outros países (MOTA; TENA, 2020).

Saiba mais

Stefano Rodotà (2008), no livro *A vida na sociedade da vigilância*, afirma que:

> [...] não se faz mais possível considerar os problemas de privacidade somente por meio de um pêndulo entre "recolhimento" e "divulgação"; entre o homem prisioneiro de seus segredos e o homem que nada tem a esconder; entre a "casa fortaleza", que glorifica a privacidade e favorece o egocentrismo, e a "casa-vitrine", que privilegia as trocas sociais; e assim por diante. Essas tendem a ser alternativas cada vez mais abstratas, visto que nelas se reflete uma forma de encarar a privacidade que negligencia justamente a necessidade de dilatar esse conceito para além de sua dimensão estritamente individualista, no âmbito da qual sempre esteve confinada pelas circunstâncias de sua origem (RODOTÀ, 2008, p. 25).

Conceitos, princípios e institutos da LGPD

A LGPD foi sancionada pensando que todo dado pessoal tem relevância e valor. Por tal razão, o conceito de dado pessoal ganhou amplitude, assim como na GDPR, no sentido de que os dados pessoais são equivalentes a informações relativas à pessoa singular identificada ou identificável, conforme preceitua o artigo 5º, I da LGPD (BRASIL, [2019]). Assim, mesmo que determinados dados pareçam não ter relevância em dado momento ou que não façam a direta referência a uma determinada pessoa, quando são transferidos, cruzados ou organizados, têm a possibilidade de resultar em dados específicos em relação a uma determinada pessoa. Eles podem carregar informações de caráter sensível sobre ela, como foi observado pelo Tribunal Constitucional Alemão no julgamento sobre a Lei do Censo em 1983 (MARTINS, 2016).

Assim, pela cautela de tratamento da matéria, a regra estabelecida pela LGPD, em seu artigo 1º, é a de que qualquer pessoa que trate de dados, seja ela natural ou jurídica, de direito público ou privado, inclusive na atividade realizada por meios eletrônicos, deverá ter um arquétipo legal para fundamentar os tratamentos de dados pessoais que realizar (BRASIL, [2019]). Portanto, não haverá necessidade de identificação de uma base legal específica apenas nos casos enquadrados nas hipóteses de exclusão da aplicação da LGPD, conforme o disposto no artigo 4º (BRASIL, [2019]). Contudo, da mesma forma, o tratamento de dados pessoais (previsto no artigo 4º, III), ou seja, aqueles para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, "[...] será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observando o devido processo legal, os princípios gerais de proteção e os direitos do titular" (BRASIL, [2019], documento *on-line*). Assim, foi estabelecida, junto à Câmara dos Deputados, uma comissão de especialistas judiciais responsáveis pela elaboração de um anteprojeto de lei em relação à matéria. Logo, quando não cabe possibilidade de exclusão, o tratamento deverá ser adaptado e realizado em pelo menos uma das hipóteses legais, para que ele seja considerado legítimo e lícito. Tais bases foram determinadas de forma genérica, e as adequações devem ser realizadas por meio da Autoridade Nacional de Proteção de Dados (ANPD), pelo Poder Judiciário e pelo Poder Legislativo (TEFFÉ; VIOLA, 2020).

É fundamental ressaltar que a LGPD no Brasil disciplina os dados por meio de fundamentos que se balizam no respeito à privacidade, na autodeterminação informativa, na liberdade de expressão, informação, de comunicação

e de opinião, na inviolabilidade da honra, da intimidade e da imagem, no desenvolvimento econômico e tecnológico, na livre iniciativa e na livre concorrência e a partir da defesa do consumidor e, de acordo com os direitos humanos, do livre desenvolvimento da personalidade e pela igualdade e exercício da cidadania pelas pessoas naturais, conforme a extração do artigo 2º, incisos I a VII, da LGPD (BRASIL, [2019]).

Vale observar que, com o advento da LGPG, uma série de conceitos foi delineada de maneira expressa, como o que acontece na definição de dados pessoais e dados sensíveis, os quais, por previsão legais, recebem tratamentos diferentes e têm determinações legislativas particulares. O artigo 5º, I, conceitua **dado pessoal** como a informação relacionada a pessoa natural identificada ou identificável, enquanto os **dados sensíveis** são aqueles relacionados a dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, além dos dados referentes à saúde ou à vida sexual, dado genético ou biométrico (quando vinculado a uma pessoa natural, disposição prevista no artigo 5º, II (BRASIL, [2019]). A lei ainda traz considerações a respeito do conceito de:

> [...] dado anonimizado [...]; banco de dados [...]; titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (BRASIL, [2019], documento *on-line*).

A base da LGPD é desenvolvida a partir da concepção de princípios e da observância da boa-fé, que regem as atividades de tratamento de dados pessoais. Por meio dos princípios que norteiam a base legal da proteção de dados, é possível compreender as condições e circunstâncias pelas quais ela vai ser aplicada, especialmente pelo fato de que os princípios funcionam como uma bússola que norteará as interpretações dos tribunais nos casos em que questões sejam aludidas e não possuam respaldo expresso no dispositivo de lei. Nesse sentido, "[...] princípio é toda norma jurídica considerada determinante de outra ou outras que lhe são subordinadas que a pressupõe, desenvolvendo e especificando o preceito em direções mais particulares" (VAINZOF, 2019, p. 136).

Assim, os princípios gerais da proteção de dados foram elaborados e expressamente previstos em lei, devendo ser interpretados em benefício do titular de dados.

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - 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;
> IV - 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;
> V - 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;
> VI - 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;
> VII - 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;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - 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 (BRASIL, [2019], documento *on-line*).

Logo, por meio do **princípio da finalidade**, o titular pode garantir a legalidade do seu processamento de dados (por meio das informações obtidas previamente, limitando a finalidade do processamento) e de terceiros, podendo ou não acessar os dado e, reduzindo, assim, o risco do uso secundário dos dados sem o consentimento do titular (VAINZOF, 2019).

O **princípio da adequação** prevê que o tratamento de dados pessoais "[...] somente pode ser realizado quando houver compatibilidade com as finalidades informadas ao titular, de acordo com o contexto do tratamento" (VAINZOF, 2019, p. 142).

A **necessidade**, como princípio previsto da LGPD, determina "[...] a limitação do tratamento aos dados pertinentes, proporcionais e não excessivos em relação à finalidade do tratamento" (LOUZADA, 2019, p. 96).

Por meio do **princípio do livre acesso**, permite-se que o titular do dado acompanhe o fluxo informacional do dado, tendo o direito de descarte em

casos de dados incorretos, desatualizados, fora de contexto ou de caráter ilícito (MACHADO; MARCONI, 2020).

O **princípio da qualidade** funciona como um instrumento de impedimento de injustiças, pois estabelece a necessidade de exatidão, clareza, relevância e atualização dos dados (LOUZADA, 2019).

O **princípio da transparência** é entendível como fonte essencial para se atingir o objetivo do instrumento legal de proteção de dados: proteger a privacidade e o livre desenvolvimento da personalidade. Sem o simples acesso às informações de forma clara e precisa em relação ao tratamento dos dados, não há como garantir ao titular a tutela da transparência (VAINZOF, 2019).

Sabidamente, o **princípio da segurança** "[...] tem relevância especial porque, em sua essência, sem segurança forte, não pode haver privacidade" (BRASIL, 2020, p. 52). Logo, a centralidade desse princípio está na manutenção dos dados da pessoa física em ambiente seguro.

O **princípio da prevenção** deve estar calcado no conceito de *privacy by design*, o qual vem sendo reconhecido mundialmente "[...] como valioso auxílio para o cumprimento de exigências legais sobre privacidade de dados, considerando que são diretrizes gerais que devem nortear o processo de adequação específica de cada empresa" (VAINZOF, 2019, p. 158).

O tratamento de dados não pode ser realizado para **fins discriminatórios** ilícitos ou abusivos.

> Não se pode ter exclusão de titulares de dados pessoais no momento de seu tratamento de dados pessoais por determinadas características, sejam elas de origem racial ou étnica, opinião política, religião ou convicções, geolocalização, filiação sindical, saúde ou orientação sexual (MACHADO; MARCONI, 2020, p. 2611).

Finalmente, por meio do **princípio da responsabilização e prestação**, a LGPD demonstrou aos controladores e aos operadores de dados que eles são responsáveis por todas as medidas que forem adotadas com o objetivo de atender a exigências legais e de princípios estabelecidos em lei (VAINZOF, 2019).

Os princípios previstos na LGPD, ainda que fracionados, condensados ou adaptados, formam a centralidade de diversas leis, tratados, convenções ou acordos de proteção de dados pessoais. Juntos, formam o núcleo das questões com as quais o ordenamento deve se deparar ao procurar fornecer sua própria solução ao problema da proteção dos dados pessoais (DONEDA, 2011).

Outra questão de extrema importância extraída da LGPD é o tratamento dos dados pessoais e dos dados sensíveis, expressamente previstos na lei de proteção de dados brasileira. Compreende-se que, tanto o rol do artigo 7º, que prevê o tratamento dos dados pessoais, quanto o do artigo 11, que

dispõe sobre o tratamento de dados sensíveis (BRASIL, [2019]), são taxativos, embora sejam dotados de hipóteses mais abertas e com relativo grau de subjetividade, como o legítimo interesse (TEFFÉ; VIOLA, 2020).

> De forma a se evitar abusos no tratamento de dados e garantir os direitos do titular, ele poderá revogar o seu consentimento, [...] ou pleitear o direito à oposição, que significa que o titular poderá se opor a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto na LGPD (Art. 18, §2º). Além disso, encontra-se positivado o direito à explicação (Art. 20), que dispõe que o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (TEFFÉ; VIOLA, 2020, p. 4-5).

O sistema legal que foi desenvolvido para o tratamento de dados confere ao titular instrumento de controle em relação as suas informações pessoais e de garantia de direitos, com especial destaque para o consentimento e o legítimo interesse. O consentimento simboliza "[...] instrumento de manifestação individual no campo dos direitos da personalidade e tem o papel de legitimar que terceiros utilizem, em alguma medida, os dados de seu titular" (TEFFÉ; VIOLA, 2020, p. 7). É por meio do consentimento que se realiza a promoção da personalidade, representando uma modalidade para a edificação e determinação da esfera privada. Ele vincula-se, então, à autodeterminação existencial e informacional do ser humano, se apresentando como fundamental para a proteção do titular dos dados e, da mesma forma, para o fluxo de informações (DONEDA, 2011).

A LGPD, na disposição do artigo 5º, XII, prevê o consentimento como a "[...] manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (BRASIL, [2019], documento *on-line*). Com relação ao consentimento requerido e ao consentimento necessário, Teffé e Viola (2020, p. 10) afirmam:

> Na hipótese em que o consentimento é requerido, ele será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca. Quando o consentimento for necessário, havendo mudanças em relação à finalidade para o tratamento dos dados não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo este revogar o consentimento, caso discorde das alterações.

Assim, a LGPD procura, seja pelo consentimento, seja pelo tratamento de dados ou por tantos outros instrumentos dispostos expressamente na

legislação, implementar mecanismos para a proteção e garantia da dignidade humana. Assim, a lei de proteção de dados, além de facilitar o controle dos dados tratados, impõe responsabilidades aos agentes de tratamento e oportuniza segurança para que as informações sejam transmitidas. A lei objetiva avançar os riscos de violação à privacidade e impede intervenções abusivas de informações e vazamento de dados (TEFFÉ; VIOLA, 2020).

Saiba mais

O estudo "Direito fundamental à liberdade de pesquisa genética e à proteção de dados pessoais: os princípios da prevenção e da precaução como garantia do direito à vida privada", de Regina Linden Ruaro (2015), analisou os direitos fundamentais de liberdade de pesquisa e da proteção de dados pessoais no âmbito da genética humana e propôs a aplicação dos princípios de precaução e da prevenção. A partir desse trabalho, foi realizada uma avaliação da legislação brasileira como medida de garantia à privacidade dos dados pessoais e das informações colhidas na investigação científica. O estudo queria elucidar a limitação de direitos fundamentais a partir da concepção de que eles não são absolutos. Foi proposta, ainda, a aplicação dos princípios da precaução e da prevenção no ciberespaço.

LGPD nas áreas de educação, saúde e relações trabalhistas

O artigo 5º, inciso II, da LGPD, traz importantes e sensíveis desdobramentos dos dados pessoais (BRASIL, [2019]). Entre eles, estão os dados vinculados com saúde, também denominados de dados clínicos ou informações médicas. Por seu elevado potencial discriminatório e lesivo, os dados que contêm informações de saúde impulsionam a imprescindibilidade de preservação e proteção, para que sejam garantidos os direitos à dignidade, ao sigilo e à vida privada dos titulares (BRASIL, [2019]).

Pelo elevado grau de lesividade dos dados sensíveis (por revelarem informações de caráter personalíssimo, embutidas no âmbito da proteção do direito de personalidade), sua coleta, processamento e tratamento devem acontecer apenas após o consentimento expresso do titular, uma vez que a inobservância da anuência viola a legislação de proteção de dados, com destaque para os dados confidenciais e as reservas do ser (SIQUEIRA; HOCH, 2019).

Há construção teórica e legislativa, no plano internacional, que fomenta a utilização do referencial de "direitos humanos dos pacientes" (DHP), previstos em documentos elaborados e adotados no âmbito de organizações e sistemas internacionais, como

> ferramenta para análise de imbróglios éticos que exsurgem na área da saúde. São considerados direitos humanos aplicáveis ao contexto dos cuidados em saúde e de pacientes o direito à vida, o direito a não ser submetido a tratamento desumano, degradante, cruel ou à tortura, o direito à liberdade e segurança pessoal, o direito à saúde integral, o direito de não sofrer discriminação de qualquer tipo, e, especialmente relevante ao presente propósito, o direito à informação e ao respeito à vida privada. Pode-se afirmar, assim, a partir da abordagem exposta, que os dados médicos revelam-se como importante ramificação dos dados pessoais e consistem em informações sensíveis de saúde depositadas em hospitais, após internações ou cirurgias, em laboratórios, após a coleta de exames, em clínicas, após a realização de procedimentos, em consultórios médicos, odontológicos, fisioterapêuticos, psicológicos ou psiquiátricos, após a realização de consultas e sessões, ou até mesmo em cadastros de planos de saúde, após a solicitação de autorização para realização de exames ou procedimentos. Além dos dados de saúde, os registros dos pacientes em citados estabelecimentos contêm inúmeras informações de cunho pessoal, incluindo nomes, datas de nascimento, endereços, números de seguro e de planos de saúde de cada indivíduo (SIQUEIRA; HOCH, 2019, p. 8).

Assim, pelo potencial interesse na coleta de dados de saúde dos titulares, não apenas por seguradoras e planos de saúde, mas também por *hackers* e estelionatários, é necessário que a participação do detentor dos dados seja efetiva. Nesse sentido, a autodeterminação informativa do paciente (fundamento essencial da LGPD) deve ser protegida a partir dos preceitos trazidos no artigo 2º, II (BRASIL, [2019]), inaugurando-se com o preenchimento do termo de consentimento esclarecido e informado, instrumento necessário tanto para a realização de uma consulta médica quanto para o desenvolvimento de pesquisas científicas. Os termos de consentimento devem "[...] conter avisos claros relativos ao grau de confiabilidade de exames, alertas de possíveis riscos, consequências fisiológicas e complicações, além do caráter, objetivos e benefícios da intervenção" (SIQUEIRA; HOCH, 2019, p. 10). Eles também devem conter linguagem simples, para que a compreensão do paciente seja completa, autônoma e consciente durante o ato de anuência ou rejeição.

Entretanto, como se trata de dado sensível, o consentimento tem expressiva importância diante dos dados médico. São escassos os termos de consentimento que advertem o paciente em relação ao uso, destino e armazenamento dos dados de saúde, o que coloca em risco o direito à privacidade e à intimidade do indivíduo.

Por outro lado, vale destacar a interferência que a publicação da LGPD trouxe para as relações trabalhistas. Embora não haja qualquer menção na lei de proteção quanto às questões que vinculam o direito do trabalho por seus dispositivos relacionados ao tratamento de dados pessoais e sensíveis, é possível se depreender que, de forma fática, aplica-se o artigo 1º, bem como

o artigo 5º, da LGPD (BRASIL, [2019]) às relações de trabalho, regulamentadas por meio da Consolidação das Leis Trabalhistas (CLT) (BRASIL, [2017]).

Assim, da análise conjunta da LGPD e da CLT, retira-se que o empregador se enquadra como agente controlador dos dados de seus funcionários, de candidatos às vagas de emprego e de funcionários desligados. Para os fins da LGPD, os dados manipulados por empregadores são compatíveis com os previstos no artigo 5º, X, da legislação de proteção de dados nacionais (BRASIL, [2019]).

> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, [2019], documento *on-line*).

Por outro lado, funcionários, candidatos às vagas de emprego e funcionários desligados são denominados titulares dos dados e detêm dados pessoais e sensíveis, como informações sobre associação a sindicatos.

> Há um intenso fluxo de "Dados Pessoais", tal qual definido na LGPD, envolvendo o contrato de trabalho, diretamente entre o Empregado-Titular e o Empregador-Controlador/Operador, desde (a) as fases anteriores à sua celebração (informações sobre o candidato, currículo, histórico, etc.), passando (b) pela celebração do contrato de trabalho (dados cadastrais, filiação a sindicado, endereço, nomes dos genitores, escolaridade, situação familiar, nomes dos filhos, idade, tipo sanguíneo etc.), e ainda (c) durante a execução do contrato de trabalho (jornada de trabalho, valor do salário, descontos, faltas, motivos das faltas, doenças, acidentes, situações conjugais que podem ter reflexos em providências da empresa, como o pagamento de pensão, inclusão de um dependente no plano de saúde, etc.), e por fim (d) ao término do contrato de trabalho (motivo do desligamento, valor das verbas rescisórias, etc.) (OLIVIERI, 2019, documento *on-line*).

Nesse caso, em que o empregado é o titular dos dados e o empregador é o controlador (uma vez que realiza o tratamento de dados fornecidos em razão do contrato de trabalho), a LGPD é aplicável para as relações de trabalho, sendo de responsabilidade do empregador verificar as regras relativas à proteção de dados pessoais de seus funcionários e aplicar medidas de segurança, técnicas e administrativas para a proteção dos dados, conforme a previsão do artigo 46 da LGPD, aplicável desde a fase de concepção do produto ou serviço até a sua execução (BRASIL, [2019]). Assim, por meio de uma interpretação extensiva, visto que se trata de norma de proteção, o empregador deve tratar adequadamente as informações dos funcionários na pré-contratual, na fase

contratual e na fase pós-contratual, por exemplo, por meio do cuidado com o termo de rescisão de contrato de trabalho (TORRES; CALCINI, 2020).

É importante destacar que, por força da LGPD, o empregador passa a ter a obrigação de informar ao titular do dado sobre a forma de tratamento desses dados, observando os princípios da licitude, lealdade e transparência, além dos previstos expressamente na lei de proteção de dados pessoais. Além disso, para a realização de tratamento lícito, o titular dos dados pessoais sensíveis deve emitir seu consentimento para as finalidades a que são propostas (GRECO, 2020).

É possível analisar também a relação entre a LGPD e a educação. Assim como nos casos das relações de trabalho e dos dados vinculados à saúde, também é necessária a adaptação dos ambientes de ensino à LGPD. Porém, o destaque especial à área da educação está no tratamento dos dados previstos no artigo 14 da LGPD, que indica o controle do tratamento dos dados pessoais de crianças e adolescentes por todas as instituições que, de alguma forma, colhem informações de menores (PINHEIRO, 2020).

O risco está no fato de que a exposição ou o vazamento de dados de menores é expressivo, uma vez que, cada vez mais cedo, os indivíduos têm acesso aos recursos digitais, seja para questões pessoais, seja como recursos de ensino e aprendizagem (PINHEIRO, 2020). Em tempos de pandemia, isso está ainda mais acentuado, pois as escolas estão fechadas e os alunos estão recebendo tratamento escolar *on-line*.

Assim, os controladores, que na educação representam majoritariamente as instituições de ensino, devem observar o que indica a LGPD em relação ao consentimento, que deve ser fornecido por um dos pais ou pelo responsável legal da criança ou do adolescente (PINHEIRO, 2020). Caso não o fizer, o controlador fica sujeito às sanções previstas na lei de proteção de dados: multas que variam de 2% do faturamento até R$ 50 milhões (BRASIL, [2019]).

> Mesmo em casos específicos, em que a instituição precise contatar os pais ou representantes legais, se não tiver o consentimento ainda, esses dados coletados só poderão ser usados para essa ação pontual, e apenas uma única vez, não sendo permitido armazená-los. Além dos dados pessoais, que identificam a criança ou o adolescente, como nome completo, dados dos pais, endereço, entre outros, há os dados sensíveis, que incluem religião, origem racial ou étnica e até informações sobre saúde, que não estão de fora das exigências tratadas na LGPD. Portanto, no caso escolar, os relatórios pedagógicos sobre o rendimento do aluno têm muitas informações que se enquadram na categoria de dados sensíveis (PINHEIRO, 2020, documento *on-line*).

Devem se adequar à LGPD, sob pena de recebimento de sanções, creches, escolas, universidades e mantenedoras sociais ou religiosas, incluindo fornecedores que atuam em conjunto com elas, como o transporte escolar, os responsáveis por passeios e excursões e até mesmo o teatro, o museu, o cinema e os ambientes que realizam atividades esportivas (PINHEIRO, 2020).

Na educação, deve-se realizar o equilíbrio entre os dados necessários, a forma de tratamento deles e tudo o que é trazido pela conveniência e pelo instrumento legal em vigor no território nacional. É importante destacar alguns pontos importantes à educação. O primeiro deles é a atualização de contratos de matrícula, que agora passam a contemplar uma demonstração clara de quais dados são coletados, onde são armazenados, por quanto tempo esse armazenamento acontecerá, quem terá acesso aos dados e qual é a finalidade de sua utilização. Para atender à LGPD, em especial ao seu artigo 14, os alunos devem ser separados por idade, a fim de verificar a necessidade de consentimento para o tratamento dos dados (BRASIL, [2019]). Por fim, investimentos em segurança de dados na educação passam a ser imprescindíveis, assim como o amparo legal para cada dado coletado, mantendo sempre uma comunicação clara com os usuários e seus pais ou responsáveis legais. Professores, secretários, diretores, gestores, reitores e todos os outros profissionais vinculados à área da educação devem passar por um treinamento adequado, para conhecer as implicações da LGPD na educação.

Exemplo

Leia os textos "Impactos da Lei de Proteção de Dados (LGPD) brasileira no uso da Computação em Nuvem", de Márcio Aurélio de Souza Fernandes *et al*. (2021), e "LGPD: o que a condenação da Cyrela por uso indevido de dados deixa de alerta", de Carlos Eduardo Vasconcellos (2020), para conferir exemplos que envolvem a LGPD.

Referências

BISSO, R. *et al*. Vazamento de dados: histórico, impacto socioeconômico e as novas leis de proteção de dados. *ReABTIC - Revista Eletrônica Argentina-Brasil de Tecnologias da* Informação e da Comunicação, v. 3, n. 1, 2020. Disponível em: https://revistas.setrem.com.br/index.php/reabtic/article/view/378/174. Acesso em: 19 abr. 2021.

BRASIL. Comitê Central de Governança de Dados. *Lei Geral de Proteção de Dados (LGPD)*: guia de boas práticas para implementação na administração pública federal. Brasília: Comitê Central de Governança de Dados, 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaLGPD.pdf. Acesso em: 19 abr. 2021.

BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil de 1988*. Brasília: Presidência da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 19 abr. 2021.

BRASIL. *Decreto-Lei n. 5.452, de 1º de maio de 1943*. Aprova a Consolidação das Leis do Trabalho. Brasília: Presidência da República, [2017]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm. Acesso em: 19 abr. 2021.

BRASIL. *Lei n. 8.078, de 11 de setembro de 1990*. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 19 abr. 2021.

BRASIL. *Lei n. 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres do uso da Internet no Brasil. Brasília: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 19 abr. 2021.

BRASIL. *Lei n. 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, [2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 19 abr. 2021.

CARVALHO, L. P.; OLIVEIRA, J. Proteção de dados e humanidades digitais no Brasil: caixas-pretas. *Revista Scientiarum Historia XII*, v. 1, n. 1, p. 1-9, 2019. Disponível em: http://revistas.hcte.ufrj.br/index.php/RevistaSH/article/view/32/28. Acesso em: 19 abr. 2021.

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico*, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315/658. Acesso em: 19 abr. 2021.

FERNANDES, M. A. S. *et al*. Impactos da Lei de Proteção de Dados (LGPD) brasileira no uso da computação em nuvem. *RISTI — Revista Ibérica de Sistemas e Tecnologias de Informação*, n. e42, p. 374-385, fev. 2021.

GRECO, E. *Os impactos da LGPD nas relações de trabalho*. Law Innovation, 2020. Disponível em: https://lawinnovation.com.br/os-impactos-da-lgpd-nas-relacoes-de-trabalho/. Acesso em: 19 abr. 2021.

LOUZADA, L. Princípios da LGPD e os bancos de perfis genéticos: instrumentalizando a garantia de direito no processo penal. *Revista do Advogado*, v. 39, n. 144, p. 90-98, nov. 2019.

MACHADO, L. C. P.; MARCONI, L. P. Estudos preliminares sobre os princípios aplicados ao tratamento de dados pessoais na Lei n. 13.709/2018 - LGPD. *In*: ENCONTRO NACIONAL DE ENSINO, PESQUISA E EXTENSÃO, 25., 2020, Presidente Prudente. *Anais* [...]. Presidente Prudente: ENEPE/Unoeste, 2020.

MARTINS. L. *Tribunal Constitucional Federal Alemão*: decisões anotadas sobre direitos fundamentais. São Paulo: Konrad-Adenauer Stiftung – KAS, 2016. v. 1: Dignidade humana. Livre desenvolvimento da personalidade, direito fundamental à vida e à integridade física e igualdade.

MOTA, I. D.; TENA, L. P. Fundamentos da LGPD: círculos concêntricos e sociedade de informação no contexto de direitos da personalidade. *Revista Jurídica*, v. 2, n. 59, p. 538-576, 2020. Disponível em: http://revista.unicuritiba.edu.br/index.php/RevJur/article/download/4330/371372603. Acesso em: 19 abr. 2021.

OLIVIERI, N. *Rotinas e contratos de trabalho serão impactados pela LGPD?* Serpro, 2019. Disponível em: https://www.serpro.gov.br/lgpd/noticias/impactos-lgpd-rotinas-trabalhistas-contrato-de-trabalho. Acesso em: 19 abr. 2021.

PEZZI, A. P. J. *A necessidade de proteção dos dados pessoais nos arquivos de consumo*: em busca da concretização do direito à privacidade. 2007. 215 f. Dissertação (Mestrado em Direito) — Universidade do Vale do Rio dos Sinos, São Leopoldo, 2007. Disponível em: http://www.repositorio.jesuita.org.br/bitstream/handle/UNISINOS/2400/necessidade%20de%20protecao.pdf?sequence=1&isAllowed=y. Acesso em: 19 abr. 2021.

PINHEIRO, P. P. *A LGPD aplicada ao cenário da educação*. Serpro, 2020. Disponível em: https://www.serpro.gov.br/lgpd/noticias/2020/educacao-lgpd. Acesso em: 19 abr. 2021.

SIQUEIRA, L. S.; HOCH, P. A. Os dados pessoais e a proteção de dados de saúde: análise a partir das iniciativas de e-saúde. *In*: Congresso Internacional de Direito e Contemporaneidade, 5., 2019, Santa Maria. *Anais* [...]. Santa Maria: UFSM, 2019. Disponível em: https://www.ufsm.br/app/uploads/sites/563/2019/09/5.2.pdf. Acesso em: 19 abr. 2021.

TEFFÉ, C. S.; VIOLA, M. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. *Civilistica.com*, v. 9, n. 1, p. 1-38, 2020. Disponível em: https://civilistica.com/wp-content/uploads1/2020/05/Teff%C3%A9-e-Viola-civilistica.com-a.9.n.1.2020-2.pdf. Acesso em: 19 abr. 2021.

TORRES, L.; CALCINI, R. Os impactos da Lei Geral de Proteção de Dados nas relações de trabalho. *Migalhas*, 18 ago. 2020. Disponível em: https://migalhas.uol.com.br/depeso/332108/os-impactos-da-lei-geral-de-protecao-dedados-nas-relacoes-de--trabalho. Acesso em: 19 abr. 2021.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). *Jornal Oficial da União Europeia*, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT. Acesso em: 19 abr. 2021.

VAINZOF, R. Disposições preliminares. *In*: MALDONADO, V. N.; BLUM, R. O. (coord.). *LGPD — Lei Geral de Proteção de Dados Comentada*. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

VASCONCELLOS, C. E. *LGPD*: o que a condenação da Cyrela por uso indevido de dados deixa de alerta. O Consumerista, 2020. Disponível em: https://www.oconsumerista.com.br/2020/10/lgpd-o-que-a-condenacao-da-cyrela-deixa-de-alerta/. Acesso em: 19 abr. 2021.

Leituras recomendadas

RODOTÀ, S. *A vida na sociedade da vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RUARO, R. L. Direito fundamental à liberdade de pesquisa genética e à proteção de dados pessoais: os princípios da prevenção e da precaução como garantia do direito à vida privada. *Revista do Direito Público*, v. 10, n. 2, p. 9-38, maio/ago. 2015. Disponível em: http://www.uel.br/revistas/uel/index.php/direitopub/article/download/22298/16895. Acesso em: 19 abr. 2021.

Fique atento

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

Conteúdo:

SAGAH
SOLUÇÕES EDUCACIONAIS INTEGRADAS

Dica do Professor

Nas últimas décadas, inúmeras são as discussões que giram em torno de regulações relativas à regulamentação da privacidade e da proteção de dados pessoais, com especial atenção ao instituto do consentimento expressado pelo titular dos dados. Nessa toada, o consentimento figura como instrumento regulatório central e núcleo de legitimidade prática desse regime protetivo. O consentimento é extraído tal qual expressão da autonomia individual e do controle do titular dos dados em torno de seus direitos de personalidade.

Porém são diversas as insuficiências do consentimento diante da tutela da privacidade e da proteção dos dados pessoais dos cidadãos em relação aos desafios sociais, com especial destaque para aqueles advindos do *big data*.

Na Dica do Professor, você conhecerá as insuficiências dos padrões de consentimento e os reflexos na autonomia dos titulares dos dados pessoais.

Aponte a câmera para o código e acesse o link do conteúdo ou clique no código para acessar.

Audiodescrição da dica do professor:

Clique aqui

Exercícios

1) **A ANPD é um órgão da administração pública direta federal do Brasil, fazendo parte da Presidência da República, com a prerrogativa de zelar pela proteção de dados pessoais e da privacidade e, acima de tudo, devendo realizar a fiscalização do cumprimento da LGPD. A instituição da ANPD como autoridade nacional independente para supervisionar o cumprimento da LGPD faz com que o Brasil esteja de acordo com o GDPR da União Europeia.**

Sobre a matéria, assinale a alterativa correta.

A) Entre as competências da ANPD está a de elaborar relatórios semestrais de gestão de suas atividades.

B) A ANPD, por ser uma autoridade independente, tem o poder de aplicar sanções penais em caso de descumprimento da LGPD.

C) Os cargos em comissão da ANPD devem ser transferidos de outros órgãos do Poder Legislativo Federal.

D) O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto por cinco membros do Poder Executivo Federal.

E) A natureza jurídica da ANPD é permanente, podendo ser alterada quando houver interesse por parte do Poder Executivo Federal.

2) **Com o advento da LGPD, a preocupação por parte de empresas e *startups* em se adequar às novas normativas legais cresceu exponencialmente e, com isso, o gerenciamento do tratamento de dados pessoais passou a ser pauta constante no ambiente corporativo.**

Em relação à temática, assinale a alternativa correta.

A) A LGPD foi omissa ao disciplinar os fundamentos de proteção de dados pessoais em matéria de livre concorrência e defesa do consumidor.

B) A disposição legal de proteção de dados brasileira é aplicável ao tratamento de dados pessoais para fins unicamente jornalísticos.

C) Operador é a pessoa natural ou jurídica a qual é responsável por tomar decisões relativas ao tratamento de dados pessoais.

D) O tratamento de dados pessoais pode ser realizado para o cumprimento de obrigação regulatória pelo controlador mediante anuência do titular dos dados.

E) O consentimento do titular dos dados pode ser anuído de maneira digital desde que aponte a manifestação de sua vontade.

3) **A LGPD cuidou dos princípios que devem ser respeitados diante da proteção de dados e, cautelosamente, abrangeu diversas formas de tratamento dos mesmos, tais como a produção, a coleta, o acesso, o processamento e o armazenamento. A lei buscou, com especial atenção, a boa-fé dos agentes que trabalham com o gerenciamento de dados pessoais, fazendo-os passar a informar aos titulares sobre o objetivo do tratamento e a forma de armazenamento dos dados.**

Com relação aos princípios da Lei Geral de Proteção de Dados, assinale a alternativa correta.

A) Pelo princípio da finalidade, o médico pode utilizar os dados de pacientes para marketing nas redes sociais, dispensando a anuência do titular dos dados.

B) Um *e-commerce* de produtos de beleza, pautando-se no princípio da adequação, pode solicitar dados de saúde de seus usuários.

C) Uma financeira de veículos, baseando-se no princípio da qualidade dos dados, pode requerer de seus clientes a atualização de dados.

D) Dados pessoais relativos à filiação a sindicato ou organização abusivos, quando colocarem em risco à ordem empresarial, são indiscriminâveis.

E) Empresas de crédito devem criar programas emergenciais, uma vez que não cabem planos de prevenção para essa natureza de serviços.

4) **A proteção da privacidade e dos dados pessoais ganhou novos contornos com os avanços tecnológicos, o amplo acesso à internet e às alterações de comportamentos sociais, impulsionadas pelo uso das redes sociais, pela troca de mensagens por meio de aplicativos, pela popularização dos *smartphones* ou, ainda, pela forma de comercializar produtos pelas plataformas virtuais. O exponencial crescimento do tratamento de dados nas redes, seja pela utilização ou armazenamento, culminou em uma série de episódios de vazamento de milhões de dados de usuários. Assim, não apenas no Brasil, mas no mundo, passou-se a se preocupar com a proteção de dados por meio de documentos legais, os quais passaram a conter**

conteúdo suficiente para proteger e responsabilizar as empresas que detêm o poder dos dados de seus clientes e usuários por meio de autuações e pagamento de multas.

Diante desse novo cenário de proteção de dados, observe assinale a alternativa correta.

A) Os Estados Unidos dispõem de regulação sobre proteção de dados válida em todo país, a California Costumer Privacy Act.

B) A legislação brasileira de proteção de dados foi baseada nas normativas legais norte-americanas de direito do consumidor.

C) A LGPD limitou o valor das multas em 75 milhões de reais por infração aos agentes de tratamento de dados.

D) A Lei do Marco Civil da Internet de 2013 foi omissa na disposição quanto à proteção de dados no ambiente virtual.

E) A GDPR é válida para os países do Espaço Econômico Europeu.

5) **A LGPD foi criada com a finalidade de prever e regulamentar questões relativas ao tratamento de dados pessoais, inclusive nos meios digitais, por pessoas físicas e jurídicas, privadas ou públicas. A aplicação da legislação é bastante ampla, impactando diversos setores da economia e das ciências jurídicas, como é o caso das relações trabalhistas.**

Sobre o uso da LGPD nas relações de trabalho, assinale a alternativa correta.

A) Na fase pré-contratual, exames de sangue, exames gestacionais e de HIV podem ser coletados pelo recrutador.

B) Do recebimento de um atestado médico contendo a identificação da doença que motivou o afastamento, o dado contido no documento é pessoal.

C) As empresas podem compartilhar os dados do funcionário com operadoras de planos de saúde, após anuência do titular, para o cumprimento de ordem judicial.

D) As informações relacionadas à filiação sindical, por se tratarem de dados pessoais, podem ser compartilhadas desde que haja consentimento do titular.

E) No ato da contratação do menor aprendiz, a empresa deverá solicitar o consentimento do fornecimento de dados pelos pais ou responsável legal.

Na prática

A aplicação da LGPD no âmbito da saúde é um genuíno marco legislativo para a segurança da informação, visto que determina a forma como as informações são coletadas e armazenadas pelas empresas no mundo digital.

A Lei no 13.709/2018 trouxe a regulamentação das relações deliberadas no ciberespaço e as consequências para eventos danosos à proteção de dados. Assim, as empresas do setor de saúde devem compreender os parâmetros legislativos, com o objetivo de ajustarem suas atividades à nova realidade trazida pela legislação brasileira específica à matéria.

Existem também outros mecanismos legais, para além da LGPD, com o objetivo de manusear, proteger e armazenar dados sensíveis relacionados com o âmbito dos serviços de saúde no Brasil.

Veja, Na Prática, como é importante a adequação da área da saúde à LGPD, a partir de exemplos trazidos de outros países que já consolidaram sanções a empresas vinculadas aos serviços de saúde por não preservarem os dados dos usuários.

Conteúdo interativo disponível na plataforma de ensino!

Saiba mais

Para ampliar o seu conhecimento a respeito desse assunto, veja abaixo as sugestões do professor:

LGPD nas relações de trabalho

Neste vídeo, assista a como a LGPD se relaciona com as relações de trabalho, ainda que nela não estejam expressas as questões trabalhistas.

Aponte a câmera para o código e acesse o link do conteúdo ou clique no código para acessar.

Jurisprudência e legislação sanitária comentadas – Lei Geral de Proteção de Dados e segurança da informação na área da saúde

Neste artigo, você irá compreender, por meio de uma análise descritiva e explicativa, de que forma a LGPD se vincula com as questões do direito à saúde.

Aponte a câmera para o código e acesse o link do conteúdo ou clique no código para acessar.

Vazamento de dados no Serasa: como se proteger?

Confira, neste vídeo, a reportagem que aborda o denominado "maior vazamento de dados da história do Brasil", no qual 223 milhões de dados pessoais foram vazados. Você verá que esse caso está sob investigação do STF e aprenderá de que forma é possível se proteger.

Aponte a câmera para o código e acesse o link do conteúdo ou clique no código para acessar.

Preservação da privacidade no enfrentamento da covid-19: dados pessoais e a pandemia global

Você lerá, neste artigo, sobre como a dificuldade de realizar diagnóstico da infecção na população em geral levou a iniciativas apoiadas em tecnologias digitais, as quais vêm sendo desenvolvidas por governos ou empresas privadas, objetivando possibilitar rastreamentos de sintomas, contatos e deslocamentos de modo a apoiar estratégias de acompanhamento e avaliação na vigilância de contágios.

Aponte a câmera para o código e acesse o link do conteúdo ou clique no código para acessar.