O QUE ESTÃO FAZENDO COM MEUS DADOS?

A importância da Lei Geral de Proteção de Dados.

Dados Internacionais de Catalogação na Publicação (CIP) - (Câmara Brasileira do Livro, SP, Brasil)

Título: O que estão fazendo com os meus dados? A importância da Lei Geral de Proteção de Dados. / coordenação Paloma Mendes Saldanha. – Recife: SerifaFina, 2019.

Vários autores;
ISNB 978-85-66599-12-1;
Prefixo Editorial: 66599;
Tipo de Suporte: E-book;
Formato Ebook: PDF.

1. Advocacia 2. Inovações 3. Tecnologia. 4. Dados. 5. Lei Geral de Proteção de dados 6. Big Data 7. ANPD 8. Inteligência Artificial. I. Saldanha, Paloma Mendes. Índices para catálogo sistemático: 1. Advocacia : Tecnologia : Direito

EDIÇÃO, REVISÃO E FINALIZAÇÃO DO E-BOOK:

- Barbara Santini Pinheiro;
- Clarice Cardim Pinheiro;
- Daniel Valença de Queiroz;
- Helio Andre Medeiros Batista;
- Joana Maria de Brito Matos;
- Josemario França de Sousa;
- Julyanne Cristine de Bulhões da Silva Nascimento;
- Leonardo Lumack do Monte Barreto;
- Paloma Mendes Saldanha;
- Rodrigo Silveira Chung.

Sumário

Prefácio

Apresento, com grande entusiasmo e indisfarçável orgulho, a obra coletiva "O que estão fazendo com os meus dados? A importância da Lei Geral de Proteção de Dados", de autoria dos membros da Comissão de Direito da Tecnologia da Informação (CDTI) da OAB/PE, comissão essa presidida por Paloma Saldanha.

Tentarei sair do lugar-comum de que os dados são os novos metais preciosos. Mas o fato é que, segundo estudos recentes, os dados coletados na era da internet já têm um valor que se aproxima do montante equivalente a todo o ouro extraído pela humanidade desde o início dos tempos. Mesmo no mundo hiperconectado em que vivemos há uma crescente preocupação com a privacidade e a segurança dos dados pessoais.

Nessa esteira é que foi sancionada a Lei no 13.709, de 14 de agosto de 2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD). Inspirada na *General Data Protection Regulation* da União Europeia, a LGPD entrará em vigor, após período de *vacatio legis*, em 16 de agosto de 2020 e trará profundas alterações na forma que os nossos dados são tratados por empresas e órgãos governamentais. Uma revolução semelhante àquela ocorrida nas relações de consumo em razão da entrada em vigor do Código de Defesa do Consumidor, em 1990, deve agora ocorrer na forma como os nossos dados são colhidos, armazenados e disponibilizados.

O presente livro traz, em linguagem acessível, mas sem perder a profundidade, temas como a proteção de dados como um direito fundamental, a eficácia da Lei Geral de Proteção de Dados (LGPD), o tratamento de dados pessoais na LGPD: transparência e dever de informação, compartilhamento de dados pelo poder público para entidades privadas, dados da saúde: a

possibilidade de compartilhamento para fins de prestação suplementar de serviços e assistência, proteção de dados em um cenário acadêmico, direito de revisão: automatizada?, dos agentes de tratamento de dados pessoais, a Autoridade Nacional de Proteção de Dados (ANPD) e, ao final, um útil e didático glossário.

Com a disponibilização deste livro, a Ordem dos Advogados do Brasil – Seccional de Pernambuco, por meio da sua CDTI, cujos integrantes desde já parabenizo e agradeço, cumpre um dúplice papel: contribuir para o constante aperfeiçoamento da advocacia frente às alterações legislativas e para o esclarecimento a toda sociedade sobre um tema de suma importância no cenário atual.

Boa leitura!

Bruno Baptista

Presidente da OAB/PE

Apresentação da Obra

Formação e transformação do jurista

Paloma Mendes Saldanha
Alexandre Saldanha

Existe um jargão que rodeia o ambiente jurídico de que o estudante de Direito nunca para de estudar, pois mesmo quando se torna um profissional dos diversos setores jurídicos haverá sempre a necessidade de atualizar e aprofundar seus conhecimentos. Ideia esta que, como qualquer outra, é passível de críticas e diversas interpretações, considerando que cada indivíduo que se aventura nos estudos jurídicos é um universo a parte e pode não confirmar a premissa trazida pelo jargão, por não querer, não ter condições, não ter acesso ou quaisquer outros motivos que impeçam a constante formação do jurista.

"Haverá sempre a necessidade de atualizar e aprofundar seus conhecimentos"

Mas, ainda que a ideia em análise talvez não traga uma conclusão necessária em forma de verdade absoluta, ela traz uma verdade em forma de exigência. Como assim? Dizer que o jurista é um ser que permanentemente estuda e atualiza seus conhecimentos representa uma esperança que isto realmente ocorra, mas afirmar que o jurista "deve" sempre reciclar seus estudos e constantemente se atualizar já evidencia uma necessidade a ser satisfeita, considerando a mutabilidade do tecido social em que as práticas jurídicas se manifestam. O sistema jurídico só possui sentido e inteligibilidade considerando suas relações com outros sistemas que, junto com ele, formam uma ordem social envolvendo padrões culturais, padrões éticos, regras morais, circunstâncias econômicas e outros elementos. Desta forma, inevitável que ocorram alterações de padrões e inevitáveis alterações no conjunto de normas jurídicas que os regem, uma vez que toda ordem sofre da possibilidade de passar por metamorfoses.

> De certo modo a evolução dos modos de vida grupal corresponde a uma série de formas de simetria e de estabilidade, o que inclui a presença de relações definidas, de padrões e de normas, coisas que afinal constituem a ordem. Essas formas evoluem, com as relações e com as normas (mais os padrões de uso e os valores e as crenças), através de modelos-de-organização que em geral crescem em complexidade, e que a antropologia e a historiografia têm mencionado como fratria, clã, tribo, cidade, Estado, império, ou como horda, nação, comunidade, sociedade. Será o caso de se poder falar, portanto, de *metamorfoses da ordem*, tanto no sentido histórico-político como no histórico-social (SALDANHA, 2003, p. 69).

Em sendo assim, a cada alteração a que passa a ordem, passa também seus padrões e, consequentemente, seu conjunto de normas (seu sistema jurídico), uma vez que este tanto funda a ordem quanto é fundado por ela.

É natural então ao Direito que ele sofra alterações em decorrência das transformações sociais, pois seu conjunto de normas deve encontrar correlatos sociais, deve encontrar valores, comportamentos, exigências que equivalham aos objetos juridicamente tutelados, e uma que tudo isto sofra alterações por fluxo histórico, a ordem normativa também será alterada. Isto porque:

> [...] a ordem jurídica constitui uma sistematização de relações, tornada inteligíveis por serem colocadas em tal ou qual posição (com mais ou menos relevo) no conjunto de preceituações possíveis. O fato de ser uma *ordem* significa que o Direito organiza preceitos e estabelece vigências oficiais segundo um plano geral, no qual a compreensão crítica encontra princípios e valores – que são fundantes – e encontra correlatos sociais que forma o "contexto" social global onde assenta a ordem jurídica (SALDANHA, 2003, p. 176).

Desta ideia de contextos em que as normas jurídicas encontram correlatos pode decorrer a ideia de continua e permanente formação do estudioso do Direito, pois se o contexto sofre alterações, os significados sociais que informam o sistema jurídico também serão alterados, e daí surge a necessidade de reinterpretar e compreender novamente o sentido do regramento dos comportamentos sociais, ou criar novos parâmetros normativos. O que, por óbvio,

deverá ser de conhecimento de quaisquer profissionais que exerce profissão em diálogo com as normas jurídicas.

"Se o contexto sofre alterações, os significados sociais que informam o sistema jurídico também serão alterados"

O conhecimento do direito, seu ensino e processo de aprendizagem não podem ser considerados como algo estável, no sentido de não serem necessariamente compreendidos fora de um contexto que está sempre em mudança, pois os comportamentos humanos assim sempre estão. Daí a ideia de permanente formação, pois o aprendizado do direito é instável, em decorrência das alterações no tecido social em que as normas jurídicas se concretizam e da insuficiência do ensino exclusivamente dogmático em informar e formar ao estudioso em suas reais necessidades de compreensão do sistema jurídico. Muito disto porque:

> [...] o Estado de Direito se constitui para além da formalização do sistema jurídico, ou seja, que sua ação legal só pode ser devidamente pensada no espaço amplo da sociedade onde a moral e a política não sejam relegadas ao plano da subjetividade ou da irracionalidade (WARAT, 2004, p. 53).

Daí temos então que o Direito só pode ser compreendido se inserido num contexto maior, envolvendo uma ordem que por sua vez envolve valores, normas de outras naturezas, infraestruturas e outros elementos. E ainda que o Direito enquanto sistema só pode ser aprendido e repassado se pensado num espaço amplo da sociedade.

E disto tudo surge a ideia da constante formação e transformação do jurista. Se o profissional do direito não se mantém atualizado, não acompanhará as mudanças na legislação civil (como novas formas de propriedade, questões de gênero, surgimento de **Direitos da personalidade**, e outros), ou na área penal (novos tipos penais, descriminalização de condutas, prisões e trânsito em julgado, etc.), também as questões constitucionais (novas conjecturas de poder, exigências

por liberdades constitucionais, as posições dos tribunais superiores e inúmeras outras), e quaisquer outras novidades que impactam o ordenamento jurídico e a prática judicial, considerando as evoluções e transformações pelas quais passam o contexto social e as ordens que dialogam com a esfera jurídica.

A obra aqui em apresentação surge neste contexto de contínua formação e transformação, muito por causa das inovações tecnológicas surgidas. Mas, e o que o desenvolvimento tecnológico tem relação com isto? Muita coisa. A cada surgimento de uma nova tecnologia, ou a cada salto evolutivo que uma determinada tecnologia dá, alteram-se padrões, expectativas e exigências.

Isto sem envolver necessariamente as tecnologias da informação. Basta imaginarmos que quando surgiu a imprensa escrita, as regras de propriedade intelectual foram alteradas, as liberdades constitucionais de informação e expressão foram redimensionadas, novos crimes surgiram, daí novas normas jurídicas se tornaram necessárias. Imaginemos ainda que ao surgir veículos automotores, normas técnicas surgiram ou foram alteradas, lógicas comerciais sofreram impactos e comportamentos sociais se relacionaram com tudo isto, surgindo novas questões e desafios ao ambiente jurídico a isto tudo associado.

"Este quase irrestrito acesso coletivo à informação pode se tornar mais uma fonte de novos problemas"

E não poderia ser diferente com as tecnologias da informação, em especial a rede mundial de computadores, ainda mais com seu ostensivo amadurecimento nas últimas décadas, lhe colocando como personagem social de alta relevância. Com o desenvolvimento da internet muitas práticas sociais passam a ocorrer em forma digital. Contemporaneamente, ela se apresenta como uma ferramenta de facilitação de diversas necessidades humanas, mas, é necessário também identificar que a rede possui altíssimo potencial para ser fonte de problemas de incalculáveis naturezas. Olhando acriticamente, a rede mundial de computadores pode ser vista como melhor instrumento possível para reunir, distribuir e compartilhar estudos, opiniões, manifestações culturais, mas, este quase irrestrito acesso coletivo

à informação pode se tornar mais uma fonte de novos problemas, do que realmente de novas soluções (LÉVY, 2011, p. 133).

Dentre as questões desafiadoras que surgem com o amadurecimento da internet como elemento do cotidiano humano está a abordagem jurídica sobre o que pode, o que não pode, o que deve ser feito com as informações que cada pessoa imersa no ambiente digital oferece, particularmente as informações de natureza pessoal, pois repercute em valores jurídicos fundamentais, como privacidade e intimidade.

Neste contexto surge a necessidade da criação de parâmetros jurídicos para tutelar o problema da gestão das informações pessoais postas em ambiente digital, ou, usando a expressão que passou a representar o problema, tutelar juridicamente a proteção dos **Dados pessoais** inseridos em ambiente digital. O desafio está em identificar qual melhor parâmetro jurídico a ser criado para controlar possíveis usos de informações pessoais inseridas no ambiente digital, isto considerando que nesta sociedade em rede, todos os dados pessoais podem ser depositados, analisados, compartilhados e usados para diversos fins. Desde o momento em que entramos numa rede social até o momento em que digitamos nosso CPF em compras realizadas por máquinas digitais, passando por material que nós mesmos postamos na internet, tudo isto pode interessar a outras pessoas, sejam quais forem suas intenções. Daí o contexto em que os sistemas jurídicos passam a identificar a necessidade de estabelecer parâmetros normativos e disto surgem as leis de proteção de dados pessoais.

"O desafio está em identificar qual melhor parâmetro jurídico"

Aqui no Brasil, este parâmetro jurídico já existe (a chamada Lei Geral de Proteção de Dados) ainda que não esteja produzindo efeitos por causa da vacância necessária para adaptação para sua implantação. Mesmo que não esteja produzindo efeitos, esta lei já provoca uma série de impactos, no sentido de discussões, debates, interpretações, expectativas e críticas. E diante de tudo isto, não há como a advocacia permanecer incólume, sendo necessário que ela se manifeste a respeito destes novos problemas, pois será dela a missão de buscar

amparo judicial para as pretensões jurídicas surgidas em relação aos dados dos cidadãos que se sintam prejudicados, que se sintam na dúvida sobre como se comportar frente a uma questão que envolve suas informações íntimas e privadas.

Com a proposta de desde já se posicionar sobre questões envolvendo a Lei Geral de Proteção de dados, de analisar e interpretar suas normas, de criticar e identificar possíveis problemas e de contribuir para a contínua formação, informação e transformação do estudioso do Direito, seja qual for a profissão, a Comissão de Direito e da Tecnologia da Informação da Ordem dos Advogados do Brasil, seccional Pernambuco lança esta obra, que nasce de um esforço coletivo, de inquietações comuns e de objetivos uniformes de todos os que colaboraram para seu desenvolvimento.

Espera-se que o leitor encontre não somente prazer (porque toda leitura tem que ser prazerosa), mas, talvez principalmente, utilidade nas leituras dos textos aqui apresentados. Isto para que possam permanecer inquietos e em formação e transformação. O que vem pela frente? Ninguém sabe. Muito provavelmente, outras obras como esta surgirão e serão necessárias. Mas vamos, por enquanto, estudar, discutir e encontrar soluções para nossas duvidosas inquietações. Parabéns a todos os colaboradores e boa leitura a todos que estiverem lendo estas palavras (seja em texto digital ou impresso...).

Paloma Mendes Saldanha
Presidente da Comissão de Direito e da Tecnologia da Informação da OAB/PE. Professora. Pesquisadora. Doutoranda e Mestre em Direito pela UNICAP. Advogada. Fundadora e CEO da PlacaMãe.Org.

Alexandre Saldanha
Membro da Comissão de Direito e da Tecnologia da Informação da OAB/PE. Professor. Pesquisador. Doutor e Mestre em Direito pela UFPE. Advogado. CCO da PlacaMãe.Org_.

Referências

- LÉVY, Pierre. **Cibercultura.** São Paulo: Ed. 34, 2011.
- SALDANHA, Nelson. **Ordem e Hermenêutica.** Rio de Janeiro: Ed. Renovar, 2003.
- WARAT, Luis Alberto. **Epistemologia e ensino do direito: o sonho acabou.** Florianópolis: Ed. Fundação Boiteux, 2004.

Capítulo 1

Proteção de dados como um Direito fundamental

Beatriz Saboya
Julyanne de Bulhões
Manoela Vasconcelos
Maria Eduarda Leite
Nívea Calado

Constituição Federal. Declaração dos Direitos do Homem. *Bill of Rights*. Quando se fala de **Direitos fundamentais**, esses três importantes diplomas são sempre mencionados como os primeiros textos normativos garantidores dessa modalidade de direitos, os quais surgiram como resposta a uma necessidade de se impor limites aos atos praticados pelo Estado e, com isso, proteger a liberdade do indivíduo e ampliar a autonomia individual.

O homem, pelo simples fato da condição humana, é titular de direitos que devem ser conhecidos e respeitados por seus semelhantes e pelo Estado. (SARLET, 2003, p.78). Essa construção conceitual se deu através da própria evolução social, que implicou na observância, pelos ordenamentos jurídicos, da necessidade de proteção da pessoa humana. Não diferente, o ordenamento brasileiro, através da **Constituição Federal** de 1988, assegurou a tutela da dignidade da pessoa humana, inclusive, estabelecendo-a como fundamento da República Federativa do Brasil.

A proteção de direitos fundamentais aos cidadãos, portanto, decorreu naturalmente da necessidade de um olhar mais atento à realidade social e aos valores essenciais para assegurar o desenvolvimento de uma vida plenamente digna aos indivíduos. Tem-se, portanto, que a Constituição Cidadã de 1988 trata, em cinco capítulos de seu Título II, dos chamados "Direitos e Garantias Fundamentais", os quais se revestem de características como imprescritibilidade, inalienabilidade, inviolabilidade, universalidade, complementaridade, entre outras.

O direito à **Privacidade** encontra-se disposto no Artigo 5º, X, da CRFB/88, e assim como os direitos à intimidade, à vida privada, à honra e à imagem que são considerados distintos e autônomos. Segundo Marques (2008), entende-se que o direito à privacidade nada mais é do que aquilo que nos preserva do conhecimento alheio, reservando-nos à nossa própria vivência. Passando para uma análise mais ampla, a privacidade está relacionada com o direito subjetivo e inerente a cada indivíduo, no qual estão inseridos o modo de vida doméstico, as relações familiares e afetivas, os hábitos, o nome, a imagem, os pensamentos e os segredos nas mais diversas situações.

"O direito à privacidade encontra-se disposto no Artigo 5º, X, da CRFB/88, e assim como os direitos à intimidade, à vida privada, à honra e à imagem que são considerados distintos e autônomos."

Nesse cenário, inclusive, a busca pela proteção aos indivíduos de eventuais agressões que lhes afetassem a sua individualidade culminou na tutela dos direitos da personalidade, entendidos atualmente como o rol aberto de garantias fundamentais, nas quais se inserem o direito à intimidade, à vida privada, à honra e à imagem. A proteção desses direitos, por sua vez, possibilita ao indivíduo o desenvolvimento livre e pleno de suas aptidões pessoais, inclusive, inserindo-se no contexto garantidor da democracia.

Acontece que os direitos da personalidade refletem uma noção inacabada da sociedade atual, uma vez que foram estabelecidos em face de um retrato social da época em que foram tutelados, o que não contempla integralmente a realidade da nossa sociedade, à qual muitos se referem como "sociedade da informação". Esta consiste em uma coletividade de indivíduos em uma economia que se orienta e se movimenta a partir dos **Dados pessoais** dos bilhões de sujeitos que estão cada vez mais conectados em um panorama global. Dados, esses, chamados de pessoais pelo fato de se referirem a signos que representam atributos de uma pessoa identificada ou identificável e, por essa razão, detém uma estreita ligação com o que há de mais intrínseco naquele indivíduo que figura como seu titular (DONEDA, 2010, p. 39).

Esses signos identificadores do cidadão (BIONE, 2019, P. 99) refletem informações inerentes a uma pessoa e, por assim dizer, são prolongamentos de um sujeito. É possível, então, concluir que os dados pessoais estão inseridos no mesmo contexto dos direitos da personalidade, os quais são reconhecidos como direitos fundamentais garantidos pela Constituição. Essa ideia se confirma quando se constata que os dados pessoais se relacionam com o seu titular, com os demais indivíduos e com o Estado do mesmo modo que a intimidade, a vida privada, a honra e a imagem. Ora, se ao entender que a tutela conferida aos direitos da personalidade se justifica pela correlação desses direitos ao ser humano e sua própria condição humana e, por assim ainda entender, que esses direitos tutelam características ou conjuntos de características que distinguem um indivíduo do outro, decerto sugere-se que um dado atrelado a uma pessoa (CPF, biometria, tipo sanguíneo, etc.) está inserido no mesmo contexto e, portanto, merece o mesmo cuidado.

"Esses signos identificadores do cidadão refletem informações inerentes a uma pessoa e, por assim dizer, são prolongamentos de um sujeito."

O fato é que não havíamos nos preparados para entender a relação dos nossos dados pessoais como força central da nossa sociedade atual. Aliás, impossível projetar as implicações dos avanços tecnológicos e sociais no contexto atual, sobretudo pela força rompante e exponencial dessas evoluções. Contudo, não podemos nos esquivar do entendimento dos sujeitos como parte fundamental aos avanços, pelo que a observância das tutelas jurídicas garantidoras do desenvolvimento pleno e digno dos indivíduos não é algo que se possa ignorar. Dados pessoais são prolongamentos de um sujeito, tal como as informações que conjecturamos no contexto dos direitos da personalidade. Por essa razão, e por estarmos diante de um fenômeno de ampla propagação de novas tecnologias e seu consequente impacto na vida em sociedade, surge a necessidade de uma reflexão ágil sobre a forma como são defendidos os direitos à privacidade dos

dados no âmbito digital, tendo em vista as cada vez mais velozes mudanças que o mundo globalizado e informacional vivencia.

Logo, não se pode perder de vista que, com os avanços tecnológicos, a internet passou a estar intrinsecamente ligada ao cotidiano das pessoas, que encontraram nesta ferramenta um revolucionário meio de trabalho, de comunicação e de entretenimento. Assim, todos os dias, novos **Aplicativo** e ***Software*** são lançados com objetivo de, por exemplo, facilitar as tarefas de seus **Usuários da internet** , tornando-as menos trabalhosas, ou de diverti-los, de forma a se tornarem indispensáveis.

Qual usuário se oporia a escolher o melhor caminho para ir do trabalho à academia, onde escutará uma seleção de suas músicas preferidas para o momento de malhação, enquanto seu relógio calcula quantas calorias foram queimadas durante o treino? Provavelmente ninguém. Essas ações são bastante comuns no tempo atual, mas é necessário entender a realidade que existe por trás da utilização em grande escala desses aplicativos e dispositivos.

O que ocorre é que, embora seja muito útil essa utilização quase que ininterrupta da internet, seus usuários tornaram-se vulneráveis às empresas que fornecem esse tipo de serviço, pois elas passaram a deter um número massivo de seus dados. É fácil perceber esse cenário ao analisar o exemplo dado acima: o aplicativo de navegação tem conhecimento da sua rotina, dos caminhos que você percorre, dos seus lugares favoritos, dos lugares que você evita; já o aplicativo de música sabe seu nome, seu endereço, sua conta bancária, as músicas que você mais escuta, as que menos escuta e em quais momentos você gosta de escutá-las; por fim, seu relógio tem informações sobre sua saúde, por onde você andou, quais são as suas mídias sociais, quais os e-mails que você leu, entre outras. Com a análise de apenas três dos inúmeros serviços utilizados no cotidiano das pessoas, já é possível perceber quão expostos estão os usuários perante as empresas criadoras dos aplicativos e

"O aplicativo de navegação tem conhecimento da sua rotina, dos caminhos que você percorre, dos seus lugares favoritos, dos lugares que você evita"

produtos eletrônicos, tendo em vista que seus dados estão sendo coletados e armazenados, muitas vezes sem o seu consentimento e o seu conhecimento. Da mesma forma, as mídias sociais, onde os usuários expõem informações da sua vida que antes eram privadas, coletam e tratam dados pessoais muitas vezes sem que haja uma efetiva compreensão, por parte do titular/usuário, do nível de violação de privacidade a que estão sendo submetidos.

Diante de tal conjuntura, os dados pessoais passaram a ter grande valor para as empresas, já que essas passaram a poder prever o comportamento de seus usuários, de modo que podem criar propagandas extremamente direcionadas para certos tipos de público, assim como vender os dados obtidos para outras empresas e, assim, ganhar bastante dinheiro com a monetização de informações que, de fato, não lhes pertencem.

"O grande desafio do mundo jurídico: o de compatibilizar a estrutura normativa do ordenamento, por muitas vezes engessada e obsoleta"

É claro que não se propõe, aqui, um boicote ao **Mundo digital**, nem se pode negar os benefícios e praticidades que muitas destas recentes tecnologias promovem. De toda forma, é essencial que se desenvolva um pensamento crítico sobre essas questões, a fim de que o aparato legislativo possa, ainda que minimamente, oferecer compatibilidade com essa nova realidade social e, mais ainda, proteger os titulares dos dados, que se encontram em clara situação de hipossuficiência frente a seus interlocutores, de eventuais abusos que venham a ser praticados neste tão recente formato de dinâmica social.

É justamente aí que está o grande desafio do mundo jurídico: o de compatibilizar a estrutura normativa do ordenamento, por muitas vezes engessada e obsoleta, aos conflitos decorrentes dessa veloz evolução tecnológica, a qual demanda que se atribuam novas roupagens interpretativas a relevantes aspectos regulatórios, a fim de que se garantam a segurança, a privacidade e a proteção dos dados dos usuários.

Por outro lado, espera-se não somente que a própria sociedade da informação, em sua atuação no mercado e na economia criativa, promova uma cultura de transparência, focando na análise de riscos e na promoção de aparatos técnicos que minimizem os possíveis impactos à segurança e à privacidade dos usuários, mas que haja, ainda, um esforço legislativo - e por que não dizer constitucional? - para que eventuais situações de violação dessas prerrogativas estejam devidamente amparadas.

Então, diante desse caráter personalíssimo dos dados pessoais aqui já destrinchados, e pelo fato de os mesmos dados exercerem relação direta com a dignidade da pessoa humana, é justo que a proteção de dados pessoais seja elevada ao patamar da mais nobre roupagem conferida pela Constituição Federal pátria, isto é, que seja inserida na esfera tutelar dos direitos fundamentais. Pois, o mundo contemporâneo, muito mais complexo e dinâmico que o nosso texto constitucional, exige que se reconheça o direito à proteção de dados como uma das modalidades de direitos fundamentais expressamente previstas, a fim de que se garanta maior efetividade à salvaguarda desse direito e, com isso, maior combatividade às situações que representem violação a tal prerrogativa. Somente assim se poderá viabilizar uma tutela efetiva aos dados pessoais na amplitude e na relevância que o assunto requer.

"O nosso texto constitucional, exige que se reconheça o direito à proteção de dados como uma das modalidades de direitos fundamentais expressamente previstas, a fim de que se garanta maior efetividade à salvaguarda desse direito e, com isso, maior combatividade às situações que representem violação a tal prerrogativa."

A legislação de proteção de dados pessoais, portanto, somente corrobora com a necessidade de resguardar os cidadãos em sua esfera íntima e privada, o que naturalmente decorreu de um olhar para o social de forma mais atenta, sobretudo para assegurar o desenvolvimento de uma vida plenamente digna aos

indivíduos. Nesse contexto, além do status de direito fundamental inerente aos dados pessoais, cuja salvaguarda é necessária, a Lei nº 13.709/18 assegura a tutela dos dados pessoais, ou seja, de direitos da personalidade, numa esfera infraconstitucional, sendo um importante marco regulatório na proteção desses direitos.

Maria Beatriz Saboya Barbosa

Advogada, Bacharela em Direito pela Universidade Federal de Pernambuco, pós-graduada pela Universidade Anhanguera-Uniderp e atualmente atendendo ao curso de Lei Geral de Proteção de Dados do Instituto de Tecnologia e Sociedade – ITS Rio. Membro da Comissão de Direito da Tecnologia e da Informação da OAB/PE. Pesquisa e produção de conteúdo na área de Privacidade e Proteção de Dados. Co-fundadora do Coletivo Essa Moça Tá Diferente.

Julyanne Cristine de Bulhões da Silva Nascimento

Bacharel em direito pela UNICAP, advogada, pós-graduanda em Legal Tech pela PUC-Minas, membro da Comissão de Direito e Tecnologia da Informação e da Comissão de Propriedade Intelectual ambas da Ordem dos advogados de Pernambuco; Co-fundadora do coletivo Essa Moça Tá Diferente.

Manoela Vasconcelos

Advogada. Pós-graduada em Direito Público pela Estácio de Sá/CERS. Bacharela em Direito pela Universidade Federal de Pernambuco (UFPE). Membro da Comissão de Direito da Tecnologia e da Informação (CDTI) da OAB/PE. Orientadora do grupo de Privacidade e Proteção de Dados do grupo de extensão Discutindo Direito e Tecnologia (DDIT) da UFPE. Alumni do Insper no Curso de Direito Digital. Cofundadora do Coletivo Essa Moça Tá Diferente. Dedica sua pesquisa à área de privacidade e proteção de dados.

Maria Eduarda Leite

Graduanda em Direito na Universidade Federal de Pernambuco (UFPE-CCJ); Membro colaboradora da Comissão de Direito e Tecnologia da Informação da OAB-PE; Participante do grupo de estudos "Smart Cities" da UPE e do grupo de extensão "Discutindo direito e tecnologia-DDIT" da UFPE.

Nívea Calado Barreto da Silva

Advogada, graduada em direito pela UNINASSAU (2014), com especialização em Direito Eletrônico pela Faculdade Estácio de Sá (2018), atualmente atuando como assistente do Tribunal de Ética e Disciplina da OAB Pernambuco e Membro da Comissão de Direito e Tecnologia da Informação da OAB-PE.

Referências

- SARLET, Ingo Wolfgang. Dignidade da Pessoa Humana e Direitos Fundamentais. In: LEITE, George Salomão (Org.). Dos Princípios Constitucionais - Considerações em torno das normas principiológicas da Constituição. São Paulo: Malheiros, 2003.
- BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento** – Rio de Janeiro: Forense, 2019.
- MARQUES, Andréa Neves Gonzaga. **Direito à Intimidade e Privacidade**, Revista Jus Vigilantibus, 23 de fevereiro de 2008.
- DONEDA, Danilo. A PROTEÇÃO DOS DADOS PESSOAIS COMO UM DIREITO FUNDAMENTAL. Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011 91

Capítulo 2

A Eficácia da Lei Geral de Proteção de Dados (LGPD)

Barbara Santini
Halan Vera Cruz
Rhaiana Valois
Rodrigo Chung
Rodrigo Galvão

Segundo *Klaus Schwab*, diretor do **Fórum Econômico Mundial**, o desenvolvimento das novas tecnologias dá-se em um nível tão rápido e integrado que nos permite consagrar o advento de uma quarta revolução industrial, que, por sua vez, promete afetar profundamente as relações sociais, econômicas e políticas. No **Mundo digital**, então, emergem termos como ***Machine Learning***, robótica, **Inteligência artificial (IA)** e internet das coisas (IoT).

E como não poderia deixar de ser, esse período caracteriza-se também pela análise massiva de grandes volumes de dados (***Big data***) – item necessário para o funcionamento de todo e qualquer modelo de aprendizagem baseado em *machine learning*, por exemplo. A partir daí extraem-se vários *insights* que podem tanto maximizar os lucros de uma empresa quanto facilitar a vida das pessoas.

A partir do acúmulo de **Dados pessoais** tem-se um coletivo de dados que nos levará a resposta, por exemplo, de quantas pessoas de 25 a 35 anos utilizam o **Aplicativo *WhatsApp*** no período das 8h às 18h. Trata-se, portanto, da era em que os dados assumem um papel de destaque nos negócios e operações do mercado global, formando a chamada *Data Driven Economy* ou Economia dirigida/orientada pelos dados.

"É marcante os inúmeros escândalos envolvendo o vazamento de dados pessoais"

Por outro lado, também é marcante os inúmeros escândalos envolvendo o **Vazamento de dados** pessoais. Diante disso, com o objetivo de coibir tais

incidentes, bem como de trazer uma maior harmonia em relação a coleta, uso e **Tratamento** dos dados pessoais e os direitos da sociedade enquanto donos de dados considerados **Direitos fundamentais**, muitos países se lançaram na árdua tarefa de regulamentar essa nova maneira de lidar com a informação. Assim, seguindo o exemplo da união europeia, o Brasil aprovou a sua ***Lei Geral de Proteção de Dados Pessoais* (LGPD)** - Lei nº 13.709, de 14 de agosto de 2018.

E quando o assunto é eficácia de uma legislação, tema deste capítulo, alguns itens devem ser levados em consideração, como por exemplo, a quantidade de utilização daquela lei nos julgados brasileiros; a repercussão e discussão sobre a temática dentro da sociedade em que a lei está inserida; os efeitos causados nas empresas daquela sociedade; as sanções trazidas pelo "andar" em desconformidade com a lei; a utilização dela como referência para formação ou criação de estatutos, contratos, demais documentos considerados necessário a formação de uma pessoa jurídica.

"Pode-se dizer que se trata de uma lei extremamente debatida, observada e utilizada."

Entretanto, a Lei Geral de Proteção de Dados Pessoais é uma lei que, hoje (dezembro de 2019), mesmo ainda não tendo entrado em vigor, suscita muitas discussões sobre eficácia. De toda forma, pode-se dizer que se trata de uma lei extremamente debatida, observada e utilizada como referência não só na elaboração ou alteração de documentos legais que determinam a constituição de uma empresa, mas também uma lei que vem sendo utilizada ou referenciada pelas pessoas físicas – no mais das vezes leigas nas questões jurídicas -, mas bem cientes de que existe um debate sobre a temática da proteção dos dados pessoais, vez que a **Cibercultura** é algo solidificado em nossa sociedade que, hoje, é conhecida por sociedade da informação, pelo crescente uso das tecnologias digitais nas suas mais variadas formas e possibilidades cotidianas.

Dessa forma, a LGPD terá como objetivo estabelecer parâmetros mais seguros e confiáveis para o processamento de dados, além de garantir maior transparência e **Privacidade** aos indivíduos.

Assim, a Lei Geral de Proteção de Dados Pessoais foi promulgada em 14 de agosto de 2018 com previsão inicial de entrada em vigor no ordenamento jurídico brasileiro, conforme antiga redação do artigo 65, "após decorridos 18 (dezoito) meses de sua publicação oficial" (15/08/2018).

Vale salientar que os artigos que tratavam da **Autoridade Nacional de Proteção de Dados – ANPD** e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, previstos nos artigos 55 ao 59, foram vetados pela Presidência da República por incorrem em vício de inconstitucionalidade do processo legislativo, por violação ao artigo 61, § 1º, II, 'e', cumulado com o artigo 37, XIX da Constituição.

Dessa forma, em 27 de dezembro de 2018, o Presidente da República, Michel Temer, editou uma Medida Provisória de nº 869, criando a Autoridade Nacional de Proteção de Dados (ANPD) e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, bem como alterou o artigo 65, que tratava da vigência, passando a prever dois prazos para a entrada em vigor dos dispositivos da lei:

- O **primeiro**, "quanto aos Artigo 55-A ao Artigo 55-K, Artigo 58-A e Artigo 58-B, no dia 28 de dezembro de 2018", que instituiu a Autoridade Nacional de Proteção de Dados (ANPD) e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade;

- E o **segundo**, para estender o prazo de 18 (dezoito) meses para 24 (vinte e quatro meses), após a data de sua publicação, quanto aos demais artigos da lei.

Não obstante, por ocasião da análise da medida provisória, o atual Presidente da República, Jair Bolsonaro, sancionou a Lei nº 13.853, de 08 de julho de 2019, com modificações em alguns dispositivos que versam sobre a Autoridade Nacional de Proteção de Dados (ANPD) e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, além de ter acrescentado o Artigo 55-L que trata das receitas da ANPD.

Para melhor compreensão do histórico legislativo, confira-se a tabela abaixo:

Vigência da Lei Geral de Proteção de Dados Pessoais (Lei 13.709, de 14 de agosto de 2018)	
Vigência inicial	18 meses a contar de sua publicação oficial *Artigos 55 ao 59 vetados
MP n° 869, de 27/12/2018	Os artigos 55-A, Artigo 55-B, Artigo 55-C, Artigo 55-D, Artigo 55-E, Artigo 55-F, Artigo 55-G, Artigo 55-H, Artigo 55-I, Artigo 55-J, Artigo 55-K, Artigo 58-A e Artigo 58-B, no dia 28 de dezembro de 2018; 24 (vinte e quatro) meses após a data de sua publicação quanto aos demais artigos
Lei n° 13.853, de 08/07/2019 (em vigor)	Dia 28 de dezembro de 2018, quanto aos artigos 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, **55-L**, 58-A e 58-B; 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos

Outro ponto de discussão é em relação à data em que a lei entrará em vigor após a sua publicação. Para resolver esse dilema, interpreta-se a Lei n° 810, de 06 de setembro de 1949, que define o ano civil, combinado com o artigo 8º, parágrafo 1º, da Lei Complementar (LC) nº 95, de 26 de fevereiro de 1998, que trata da elaboração, redação, alteração e consolidação de leis.

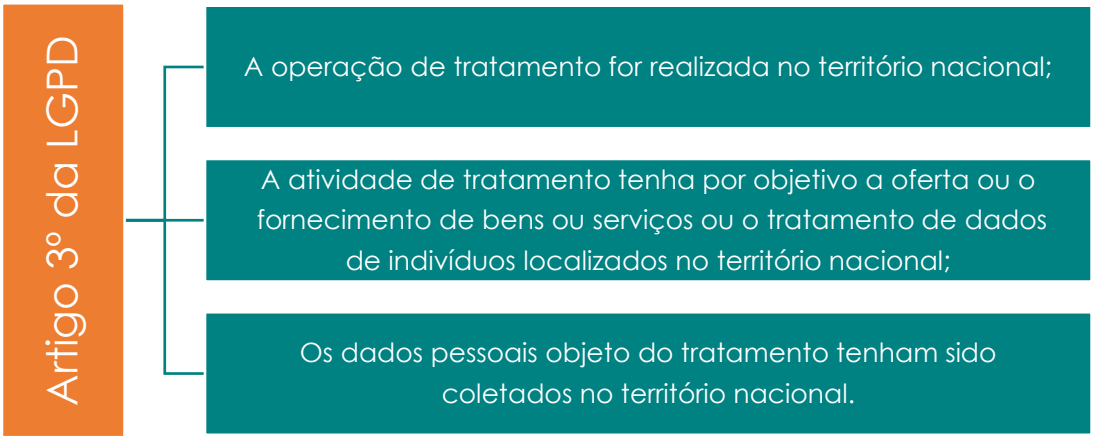
Consoante a LC 95, o prazo para leis que tem período de espera (vacância) para entrar em vigor começa a contar da data da publicação até o último dia do prazo, isto é, as leis começam a valer um dia depois de sua consumação integral.

Logo, considerando que a Lei nº 13.709 foi sancionada no dia de 14 de agosto de 2018 e foi publicada no Diário Oficial da União no dia 15, compreende-se que a lei entrou em vigor no dia 28 de dezembro de 2018 para os artigos 55-A ao 58-B, que tratam da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, e entrará em vigor no dia 16 de agosto de 2020, para os demais artigos.

O quadro sinóptico abaixo permite uma melhor visualização das datas específicas dos dispositivos da LGPD:

Vigência da LGPD	
Artigos 55-A ao 58-B (Autoridade Nacional de Proteção de Dados e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade)	28 de dezembro de 2018 (Artigo 65, I)
Demais artigos	16 de agosto de 2020 (Artigo 65, II)

É importante destacar o artigo 3º da LGPD, o qual afirma que a referida Lei aplica-se a qualquer operação de **Tratamento** realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, listando, por conseguinte, algumas condicionantes para a sua aplicação. Segundo o referido artigo, aplica-se a referida Lei, desde que:



A partir das informações trazidas acima por meio do infográfico, pode-se observar que a LGPD repercutirá diretamente no meio corporativo, sobretudo

porque os seus destinatários são pessoas físicas ou jurídicas que realizem a captação e tratamento de dados pessoais de terceiros em solo nacional.

Além disso, embora numa primeira análise pareça que a LGPD trata tão somente de proteção de dados em meios digitais, a referida Lei aplica-se também às situações em que há a captação e tratamento de dados por outros meios que não os meios digitais, como por exemplo, os cadastros físicos realizados nas empresas de diferentes ramos e seguimentos.

"A LGPD repercutirá diretamente no meio corporativo, sobretudo porque os seus destinatários são pessoas físicas ou jurídicas que realizem a captação e tratamento de dados pessoais de terceiros em solo nacional"

A LGPD impactará ou já está impactando profundamente em todos os setores da economia, trazendo modificações tanto para o âmbito privado quanto para o público, inclusive extraterritorialmente, quando especifica que todas as operações de coleta e/ou tratamento dos dados pessoais realizados no Brasil que visem a oferta de bens ou serviços em nosso território ou que tenha por objeto dados de brasileiros estarão sujeitas à lei. As empresas, portanto, independentemente de gerenciarem as informações coletadas através do arquivamento de documentos físicos ou de sistema digitais, deverão se adaptar aos novos padrões de segurança e de privacidade sob pena de, conforme o artigo 52:

a) **Advertência**, com indicação de prazo para adoção de medidas corretivas;
b) **Multa simples**, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
c) **Multa diária**, observado o limite total a que se refere o inciso II;
d) **Publicização da infração** após devidamente apurada e confirmada a sua ocorrência;

e) **Bloqueio dos dados pessoais** a que se refere a infração até a sua regularização;
f) **Eliminação dos dados pessoais** a que se refere a infração.

As sanções são rigorosas e merecem atenção. Porém, para que atinjam sua eficácia, só deverão ser aplicadas após o procedimento administrativo que possibilite a oportunidade da ampla defesa de forma gradativa, isolada ou cumulativa. Tudo de acordo com as peculiaridades do caso concreto apresentado, bem como a partir da observância de determinados parâmetros e critérios, como:

- a gravidade e a natureza das infrações e dos direitos pessoais afetados;
- a boa-fé do infrator;
- a vantagem auferida ou pretendida pelo infrator;
- a condição econômica do infrator;
- a reincidência;
- o grau do dano;
- a cooperação do infrator;
- a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do Artigo 48 da LGPD;
- a adoção de política de boas práticas e governança;
- a pronta adoção de medidas corretivas; e
- a proporcionalidade entre a gravidade da falta e a intensidade da **Sanção**.

Dessa forma, passando por todo o procedimento administrativo, possibilitando a ampla defesa e respeitando os determinados parâmetros e critérios supracitados, as sanções da LGPD podem ser aplicadas de forma correta.

Nesse contexto, pequenas e médias empresas, bem como as chamadas ***Startups***, tendem a ser as mais afetadas com a vigência dessa nova lei, pois a interrupção dos seus negócios e as sanções aplicadas podem significar um grande prejuízo.

O Artigo 46 a Lei estabelece que:

> **"Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito".**

Dessa maneira, pela análise do dispositivo depreende-se a importância atribuída à adoção de práticas de gestão e proteção de dados, que garantam o cumprimento dos requisitos mínimos exigidos pela lei. Nesse sentido, a Organização Internacional para Padronização (em inglês, *International Organization for Standardization*), conhecida como ISO, pode auxiliar muitas empresas no processo de execução dessas diretivas, vez que fornece padrões e métricas, reconhecidas e validadas internacionalmente para nortear a implementação de um Sistema de Gestão de Segurança da Informação (SGSI), aplicáveis a todos os tipos e tamanhos de organizações.

Dentre essas diretrizes, as normas da família ISO 27000 - recentemente atualizadas conforme as determinações do ***GDPR - General Data Protection Regulation*** da União Europeia -, estabelecem orientações essenciais para a melhoria da segurança e para a contenção dos riscos relacionados à utilização dados pessoais. Cabe salientar ainda que a ISO 27001 é a mais importante norma da família nesse cenário.

A partir da aplicação das normatizações estabelecidas pela ISO, portanto, a empresa estará apta a obter certificações, as quais atestam o alinhamento com as melhores práticas de manejo de informações, demonstrando, ainda, o comprometimento na proteção dos direitos individuais dos cidadãos, o que traz reflexos positivos para imagem e para credibilidade da empresa.

O cumprimento das determinações advindas dessa lei exige, então, um trabalho complexo das empresas. Isto porque terão que investir na elaboração de novas estratégias de negócios, na atualização de seus sistemas e na contratação de recursos. Além disso, deverão rever suas políticas de relacionamento com os

consumidores e fornecedores, bem como práticas de RH e marketing e até mesmo corrigir a postura de seus colaboradores.

Nesse sentido, princípios como ***Privacy by design*** e ***Privacy by default*** ganham destaque, pois se torna cada vez mais urgente repensar a arquitetura das atividades que envolvam direta ou indiretamente o manuseio de dados. Principalmente aos considerados **Dados sensíveis** (isto é, aqueles que versam sobre a origem racial ou étnica, a convicção religiosa, a opinião política, a filiação a sindicato ou a organização de caráter religioso, filosófico ou político, referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural), incorporando assim medidas de segurança e privacidade em todas as fases da cadeia de produção de bens e serviços.

Diante desse novo paradigma de **Segurança de dados**, cabe destacar a especial atenção que essas empresas e escritórios terão que despender na revisão e atualização dos contratos e documentos jurídicos para que se alinhem aos parâmetros de confidencialidade e transparência definidos pela lei. Assim, é fundamental promover a verificação das suas cláusulas contratuais, as atualizações dos seus **Termos e condições de uso**, bem como das suas **Política de privacidade** . Além disso, deve-se desenvolver ações estratégicas para o gerenciamento seguro e integrado dos contratos e repensar sua estrutura com intuito facilitar o entendimento daqueles que irão ceder seus dados.

"Empresas e escritórios terão que despender na revisão e atualização dos contratos e documentos jurídicos para que se alinhem aos parâmetros de confidencialidade e transparência definidos pela lei."

Nessa etapa, é interessante incorporar os fundamentos do chamado *legal* ***Design thinking***, processo centrado no ser humano que, de maneira inovadora, busca soluções de problemas jurídicos através da empatia. Assim, a partir de uma abordagem mais criativa, pode-se reinventar o formato tradicional dos contratos a fim de que seus termos sejam expressos de forma mais clara e objetiva.

Ademais, não se pode deixar de mencionar o papel central que o consentimento ocupa entre os fundamentos da LGPD. Tanto que, diferentemente do Código Civil que prevê apenas anulação no caso de vício de consentimento, a Lei Geral de Proteção de Dados sanciona, no Artigo 9º, §1º, a mesma hipótese com nulidade. Em consequência disso, as empresas devem se esforçar para que os seus contratos sejam um instrumento efetivo de esclarecimento e, dessa forma, a anuência dos titulares dos dados seja livre e consciente. Para isso, é importante que constem nos contratos, por exemplo, considerações sobre a forma, a duração e a finalidade específica do tratamento e/ou **Compartilhamento de dados**, além de informações acerca do **Controlador de Dados**, dos direitos do titular e das responsabilidades dos agentes que realizarão o tratamento.

Apesar de trazer inúmeras mudanças na maneira como as empresas estavam acostumadas a lidar com os dados, seguir a legislação significa construir um cenário de maior segurança jurídica para a governança de dados no Brasil. Nesse sentido, as normatizações da **ISO** podem auxiliar nesse processo de adaptação, garantindo um melhor alinhamento às práticas necessárias para a proteção das informações pessoais coletadas.

"Seguir a legislação significa construir um cenário de maior segurança jurídica para a governança de dados no Brasil."

Percebe-se, ainda, o papel relevante que os contratos representam na adequação das empresas ao texto legal, sendo profundamente afetados tanto em sua forma quanto em seu conteúdo. A LGPD, dessa forma, pode trazer inúmeros benefícios para as empresas que estiverem dispostas a se adequar e atentas as oportunidades criadas nesse novo contexto. A eficácia da aplicação dessa lei será, portanto, resultado do trabalho conjunto do governo, das empresas e da sociedade civil.

Barbara Santini Pinheiro

Advogada. Graduada em Direito pela Universidade Católica de Pernambuco (UNICAP). Pesquisadora do PlacaMae.Org_. Pós-graduanda em Direito Civil e Processo Civil pela ESA. Membro da Comissão de Direito e Tecnologia da Informação da OAB-PE.

Halan Santos Vera Cruz

Advogado e Consultor especializado na área trabalhista empresarial; Membro da Comissão de Direito da Tecnologia da Informação da OAB/PE; Pesquisador na área da tecnologia da informação e sua influência nas relações de trabalho.

Rhaiana Valois
Graduanda em Direito pela Universidade Federal de Pernambuco. Membro da Comissão de Direito da Tecnologia e da Informação da OAB/PE.

Rodrigo Silveira Chung
Presidente da Associação de Defesa de Direitos Digitais (ADDD), membro da Comissão de Direito de Tecnologia e da Informação (CDTI) da OAB/PE, advogado.

Rodrigo Galvão
Bacharel em Direito pela Faculdade Pernambucana de Cultura e Ensino – SOPECE (2006); Especialização/MBA em Direito Empresarial pela Fundação Getúlio Vargas – FGV; Pós-graduação em Processo Civil pela Faculdade do São Francisco – FACESF; Professor da Pós Graduação do Instituto dos Magistrados do Nordeste – IMN; Diretor do Instituto Brasileiro de Direito da Informática – IBDI; Diretor e Fundador da Associação de Defesa dos Direitos Digitais – ADDD..

Referências

- ANDRADE, Vitor Morais de; HE, Stella Jin Kim. Possuir a certificação ISO/IEC 27001:2013 significa estar Compliance com a LGPD?. E quais as expectativas para a ISO/IEC 27701:2019? A questão do consentimento na Lei Geral de Proteção de Dados. Consultor Jurídico, 2019. Disponível em: https://www.migalhas.com.br/dePeso/16,MI309466,71043Possuir+a+certificacao+ISOIEC+270012013+significa+estar+Compliance. Acesso em: 04 de outubro de 2019.
- BRASIL, **Lei n° 13.709**, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em 11 de outubro de 2019.
- BRASIL, **Medida Provisória n° 869**, de 27 de dezembro de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Mpv/mpv869.htm. Acesso em 02 de outubro de 2019.
- BRASIL, **Lei n° 810**, 6 de setembro de 1949. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/1930-1949/L810-49.htm. Acesso em 11 de outubro de 2019.
- BRASIL, **Lei Complementar n° 95**, de 26 de fevereiro de 1998. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp95.htm. Acesso em 11 de outubro de 2019.
- BRASIL, **Lei n° 13.853**, de 8 julho de 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm. Acesso em 11 de outubro de 2019.
- CIPRIANO; Antônio. **LGPD e Assessment: abordagem favorece preparação integral para novas regras.** Tiinside, 2019. Disponível em: https://www.advogatech.com.br/blog/@HenriqueDantas/lgpd-o-que-e-privacy-by-design-e-privacy-by-default-vc4zyjv. Acesso em: 13 de setembro de 2019.
- DANTAS; Henrique. LGPD: **O que é Privacy by Design e Privacy by Default**. Advogatech, 2019. Disponível em: https://tiinside.com.br/24/11/2019/lgpd-e-assessment-abordagem-favorece-preparacao-integral-para-novas-regras-2/. Acesso em: 13 de setembro de 2019.
- LEONEL, Guilherme; MIYAZAKI, Natalia. **Legal Design — Uma nova forma de pensar o Direito**. Medium, 2018. Disponível em: https://medium.com/@legalhackerscampinas/legal-design-uma-nova-forma-de-pensar-o-direito-c2618acbfd99. Acesso: 10 de setembro de 2019.
- **Lei Geral de Proteção de Dados: impactos e mudanças no uso e na coleta de dados pessoais.** Thomson Reuters Legal One, 2019. Disponível em:

https://www.thomsonreuters.com.br/content/dam/openweb/documents/pdf/Brazil/white-paper/thomson-reuters-legal-whitepaper-lei-geral-de-protecao-de-dados.pdf. Acesso em: 13 de setembro de 2019.

- **O que é Legal Design Thinking e como pode ajudar a rotina de um Advogado.** Certisign Explica, 2019. Disponível em: https://blog.certisign.com.br/o-que-e-legal-design-thinking-e-como-pode-ajudar-a-rotina-de-um-advogado/. Acesso em: 10 de setembro de 2019.
- SCHWAB, Klaus. **The Fourth Industrial Revolution: what it means, how to respond**. The World Economic Forum. Disponível em: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/ .Acesso em: 30 de agosto 2019.
- SOARES; Pedro. A questão do consentimento na Lei Geral de Proteção de Dados. Consultor Jurídico, 2019. Disponível em: https://www.conjur.com.br/2019-mai-11/pedro-soares-questao-consentimento-lei-protecao-dados. Acesso em: 10 de setembro de 2019.

Capítulo 3

O tratamento de dados pessoais na LGPD: transparência e dever de informação

Ana Paula Canto
Gabriela Caio
Manoela Vasconcelos
Maria Beatriz
Raquel Melo
Yanne Holanda

Para além do feito de conectar pessoas, a **Revolução Digital** que a contemporaneidade vivencia é notadamente marcada pela formação de conexões inteligentes entre pessoas, pessoas e coisas, ou mesmo entre coisas e coisas (NASCIMENTO, 2015). Nesse contexto, além da profunda mudança de sociabilidade, uma das grandes características desta nova dinâmica reside numa crescente participação de agentes não humanos nas mais variadas atividades do cotidiano: máquinas, sensores, **Algoritmos** e dispositivos conectados à Internet assumem o protagonismo das cadeias relacionais, exercendo funções cada vez mais relevantes na vida em coletividade.

Como decorrência direta deste fenômeno, usualmente chamado de hiperconectividade, uma quantidade astronômica de **Dados pessoais** é diariamente coletada, processada, compartilhada, tratada e armazenada em bancos de dados utilizados pelas empresas de tecnologia para as mais diversas finalidades, o que caracteriza a recente figura do ***Big data*** como sendo de imensa valia ao **Mercado *tech*** .

A esse respeito, vale trazer as palavras de Maike Wile (2017), para quem

> "O *Big Data* é mais que um emaranhado de dados, pois é essencialmente relacional. Isso não é novo - para a tristeza daqueles que acreditam que a internet mudou todas as coisas. O que a internet fez foi dar uma nova dimensão a esse fenômeno, transformando-o. **Para bem entender essas transformações, precisamos compreender que o *Big Data* somos nós**." (grifos acrescidos)

Uma vez que este bombardeio de inovações tecnológicas e o crescente fluxo de informações representam um relevante componente transformador da vida em sociedade, aumenta também a necessidade de se compreender as repercussões jurídicas advindas deste cenário, sobretudo no que concerne aos deveres de transparência e de informação adequada aos **titulares** desses dados.

Nesse sentido, o primeiro grande esteio do ordenamento jurídico brasileiro a tratar do dever de informação foi justamente a **Constituição Federal** de 1988, que instituiu, em seu artigo 5º, inciso, XIV[1], o direito fundamental à informação, sendo este alicerçado em três pilares dimensionais: o direito de informar, o direito de se informar e o direito de ser informado. De se considerar, ainda, que o direito à informação recebe abordagem constitucional mais específica quando a informação pretendida constar de banco de dados, cadastros públicos ou cadastros de caráter público, nos termos do Artigo 5º, inciso XXXIII da Carta Magna[2].

"O direito fundamental à Informação... (é) ...alicerçado em três pilares dimensionais: o direito de informar, o direito de se informar e o direito de ser informado."

Mais especificamente no que tange à legislação consumerista pátria, o **Código de Defesa do Consumidor** (Lei nº 9.078, de 11 de setembro de 1990) traçou importantes delimitações quanto à **Privacidade** e à segurança dos consumidores, estabelecendo uma Política Nacional das Relações de Consumo que deve viabilizar a transparência e a proteção dos interesses dos consumidores. Atendendo os princípios da "educação e informação de fornecedores e consumidores, quanto aos seus direitos e deveres, com vistas à melhoria do mercado de consumo".

---

1 *Artigo 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...)*
XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;
2 *XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado;*

No mesmo sentido, são elencados, no Artigo 6º do mesmo diploma legal, como direitos básicos do consumidor os seguintes:

> "III - A informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem;
> IV - A proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais, bem como contra práticas e cláusulas abusivas ou impostas no fornecimento de produtos e serviços; (...)"

Não se pode esquecer, ademais, a disposição contida no Artigo 43 da supramencionada Lei[3], por meio da qual ao consumidor resta assegurado o acesso às informações sobre ele armazenadas em cadastros e bases de dados, não sendo demais afirmar, por conseguinte, que do Código de Defesa do Consumidor emanam as principais diretrizes norteadoras do que veio a sedimentar, posteriormente, uma legislação específica destinada à proteção dos dados pessoais (***Lei Geral de Proteção de Dados Pessoais* - LGPD**).

O próprio Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014), por seu turno, assegura aos **Usuários da internet** o direito a informações claras sobre as etapas de coleta, uso, armazenamento, **Tratamento** e proteção de seus dados pessoais, dando claros contornos às condutas que deveriam observar as empresas de tecnologia ao manipular tão massivo volume de informações.

"O próprio Marco Civil da Internet (...), assegura aos usuários da internet o direito a informações claras sobre as etapas de coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais"

Percebe-se, portanto, que a LGPD - em que pese representar grande avanço legislativo no caminho do fortalecimento regulatório dado à matéria, bem como da efetividade das

3 Artigo 43. O consumidor, sem prejuízo do disposto no Artigo 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

"Os dados pessoais são informações pertencentes a alguém, informações relacionadas a identificação ou a possibilidade de identificação de alguém, de modo individualizado"

noções de privacidade e proteção de dados pessoais - , em muitos momentos, reflete bases axiomáticas já existentes em nosso ordenamento jurídico, o que indica que já se verifica, no Brasil, uma consciência principiológica, ainda que embrionária, quanto à necessidade de salvaguarda dos direitos inerentes aos dados e a seus titulares frente a eventuais violações de suas premissas.

A proteção dos dados pessoais no Brasil, portanto, é embasada por um forte arcabouço legal, de forma que, com a entrada em vigor da LGPD, já é possível estabelecer meios eficazes para proteção destes dados. É importante entender que essa proteção é, de fato, necessária, uma vez que, em função do *Big Data*, os cidadãos foram postos em uma situação de vulnerabilidade e hipossuficiência frente às empresas que detêm e utilizam os seus dados para fins comerciais.

"Os dados sensíveis são aqueles dados que podem gerar distinção e discriminação do seu titular pela sua caracterização."

Os titulares foram privados da **Autonomia informativa** sobre seus próprios dados, ou seja, foi tirada deles a possibilidade de determinar quem possuirá, quem tratará e para qual fim serão utilizados os seus dados. Esse controle do titular dos dados sobre as suas informações consiste na autodeterminação informativa e esta é fundamental para que o tratamento dos dados se dê de maneira transparente.

Os dados pessoais são informações pertencentes a alguém, informações relacionadas a identificação ou a possibilidade de identificação de alguém, de modo individualizado. Por sua vez, os **Dados sensíveis** são aqueles dados que podem gerar distinção e discriminação do seu titular pela sua caracterização. Sendo os dados pessoais e os dados sensíveis informações tão importantes sobre o

indivíduo, como bem explicado nos capítulos anteriores, faz-se necessário resguardar a sua proteção e exigir a transparência em seu tratamento.

É diante desta perspectiva de retomada da titularidade de dados pessoais que a LGPD introduz em nosso ordenamento jurídico uma gama de direitos aos titulares de informações pautados nos **Direitos fundamentais** de liberdade, de intimidade e de privacidade, a fim de equilibrar o relacionamento entre estes titulares e os **Controlador de Dados**. Neste sentido, o Capítulo III do dispositivo legal ora em análise, traz estes direitos discriminados.

Em linhas gerais, aos titulares é reconhecido o direito de obterem informações sobre o tratamento e uso dos seus dados pelo controlador, a qualquer tempo e por meio de requisição (caput, Artigo 18) – cujo pedido será feito diretamente ao agente de tratamento e sem custo ao requerente (§ 5º, Artigo 19). Estes mecanismos propostos na LGPD buscam permitir ao titular dispor, de fato, sobre seus dados pessoais e sensíveis.

É importante ressaltar, também, que o texto legal determina que a coleta de dados pessoais referentes ao exercício regular de direitos não pode ser utilizada em prejuízo do titular (Artigo 21), devendo serem usados apenas para a finalidade para qual foram coletados.

Mais especificamente, a LGPD prevê, em seu artigo 18, nove modalidades de direitos do titular de dados. Desta forma, a partir da nova legislação qualquer pessoa poderá requerer a confirmação de uso ou tratamento de seus dados pelo agente de tratamento (inciso I, Artigo 18), bem como o acesso a esses dados (inciso II, Artigo 18) e a realização de correções em caso de informações incompletas, inexatas ou desatualizadas (inciso III, Artigo 18).

Poderá ser requerida pelo titular a **anonimização** - processo de desvinculação do dado a uma pessoa específica e identificável -, o bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD (inciso IV, Artigo 18).

O compartilhamento dos dados coletados com entidades públicas e privadas também poderá ensejar requerimento de informação (inciso VII, Artigo 18), permitindo ao titular ter noção do alcance e do uso de seus dados pessoais. O titular também terá o direito de solicitar a **portabilidade de dados** a outro

fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da **Autoridade Nacional**, observados os segredos comercial e industrial (inciso V, Artigo 18), ressalvados os dados que já tenham sido anonimizados pelo controlador (§ 7º, Artigo 18).

Com relação ao **consentimento** do uso de dados aos agentes de tratamento, qualquer pessoa poderá solicitar a eliminação de informações pessoais, desde que observadas as exceções previstas na lei (inciso VI, Artigo 18), como também poderá requerer informações sobre a possibilidade de não fornecer consentimento e quais seriam as consequências desta recusa (inciso VIII, Artigo 18), sendo um direito do titular, assim, restringir o tratamento dos seus dados. Além disso, tem-se pontuado no texto legal que é direito do titular a revogação do seu consentimento, a qualquer tempo, desde que manifestado de forma expressa (inciso IX, Artigo 18).

"Com o advento da LGPD, foram estabelecidas algumas regras para a coleta e uso de informações pessoais."

Vale destacar que os titulares podem pleitear tais direitos de forma administrativa junto à agência reguladora de dados pessoais (§ 1º, Artigo 18), criada pela LGPD, e perante os organismos de defesa de consumidor (§ 8º, Artigo 18). Caso prefira, o titular ainda poderá requerer a defesa destes direitos em juízo de forma individual ou coletiva (Artigo 22).

Com o advento da LGPD, foram estabelecidas algumas regras para a coleta e uso de informações pessoais, ou seja, ficara determinada a criação de agentes responsáveis pelo tratamento dos dados coletados. São eles: o **controlador** e **operador de dados**, figuras que estão bem trabalhadas no capítulo 8 deste livro. Entretanto, cabe aqui mencionar que as atividades de tratamento de dados pessoais, inerentes ao controlador, operador de dados e encarregado, deverão observar a boa-fé e os seguintes princípios: finalidade, adequação, necessidade, livre acesso, qualidade de dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas. Tudo em

prol da transparência e da necessidade de informação, que é um direito daquele considerado usuário da aplicação, do site, etc.

Nota-se, portanto, que o consentimento, mencionado mais acima, é apenas uma das dez bases legais que autoriza o tratamento de dados. As hipóteses descritas nos incisos II a X do artigo 5º da LGPD, **Rol taxativo** , dispensam o consentimento, de modo a retirar do titular o poder de dispor plenamente sobre seus dados. Na redação do artigo 7º, em ordem de disposição dos incisos, tem-se incialmente a autorização de tratamento em função de consentimento, que conforme o inciso XII do artigo 5º da LGPD é a manifestação livre, informada e inequívoca. Ou seja, os titulares devem ter direito a escolha efetiva acerca de que dados desejam autorizar o tratamento, ser informados dos riscos que podem estar sujeitos, bem como das medidas que serão tomadas pelos agentes de tratamento para mitigar esses riscos. Por fim, devem assentir inequivocamente ao tratamento, sendo o tratamento baseado em silêncio ou negativa do titular – ausência de consentimento expresso – ilegítimo.

A segunda base legal na qual pode se fundar o tratamento de dados, a partir da qual não mais se verificará o consentimento, é o cumprimento de obrigação legal ou regulatória por parte do controlador. Compreende-se como obrigação *in casu* aquelas previstas em leis federais, estaduais ou municipais, bem como decretos, resoluções, determinações internacionais, entre outros, excluídas as obrigações contratuais.

"Os titulares devem ter direito a escolha efetiva acerca de que dados desejam autorizar o tratamento."

O inciso II acaba de sobrepor o cumprimento de obrigações junto ao poder público ao direito do titular de dispor livremente sobre os dados, já que escusa o consentimento para privilegiar a adequação dos agentes de tratamento às disposições legais. Então, acompanhando esta lógica de privilegiar as instituições públicas, o inciso III, do Artigo 7º, autoriza o tratamento de dados pessoais pela administração pública, inclusive para o uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres. Assim, desde

que com o fito de executar políticas públicas – conceito extenso e impreciso, que se relaciona a "melhorias" destinadas a sociedade - poderá o poder público proceder com o **Compartilhamento de dados** necessários, observado o Capítulo IV da Lei Geral de Proteção de Dados. Tendo em vista a disparidade e assimetria de informação natural entre o Estado e seus governados, o Capítulo IV do diploma legal em comento trata exclusivamente do tratamento pelo poder público, que aqui, neste livro, você encontrará mais informações no capítulo 4.

Seguindo pela extensão do artigo 7º da Lei Geral de Proteção de Dados, vê-se a possibilidade de tratamento de dados pessoais quando necessária execução de contrato ou de procedimentos pré-contratuais, desde que a pedido do titular dos dados. No inciso V, retoma o titular parte de sua autodeterminação, já que, a rigor, autoriza o tratamento, necessário a contrair contrato de seu interesse. O inciso VI traz como base legal o exercício regular de direitos em processo judicial, administrativo ou arbitral. Entende-se que esta possibilidade de tratamento se funda nas previsões constitucionais de inafastabilidade da apreciação pelo Poder Judiciário (inciso XXXV, do artigo 5º) e ampla defesa e contraditório (inciso LV, do artigo 5º).

Nesse sentido, é possível armazenar dados necessários a fundar direitos em demandas gerais, devendo ser observados os prazos prescricionais dispostos nos diplomas legais que baseiam esse direito a fim de não deslegitimar o tratamento em função da ausência de finalidade.

Está autorizado ainda o tratamento de dados sem consentimento para proteção da vida ou da incolumidade física do titular ou de terceiros. Lima e Maldonado (2019, p. 185) trazem como exemplo:

> "A obtenção de dados de geolocalização de dispositivos de telefone celular, com o objetivo de tentar localizar eventuais vidas que possam estar no meio dos escombros, após determinado incidente. Igualmente, situações em que pessoas possam ter sido sequestradas ou estejam perdidas das suas famílias podem ensejar tentativas de obtenção de dados de geolocalização, a fim de identificar os titulares."

O inciso VII, por sua vez, garante o tratamento de dados para tutela da saúde, em procedimento realizado por profissionais da área de saúde ou por

entidades sanitárias, já que os dados dos pacientes – aqui traduzidos em histórico médico – são indispensáveis ao tratamento direcionado e melhor tutela da saúde. Assim, está autorizado o tratamento com fundamento nesta base legal, vedados outros usos que desvirtuem essa finalidade.

Dados pessoais podem ser tratados, ainda, para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. Quanto a esta base legal, restam obscuras as questões que envolvem os limites do tratamento por interesse legítimo de terceiro, diante da indefinição da legislação a esse respeito, que se dedica em seu artigo 10º em tratar unicamente do tratamento pela figura do controlador. Por fim, está autorizado o tratamento de dados pessoais para proteção de crédito. Para tanto, deve ser observado o disposto na **Lei do Cadastro Positivo** e o Código de Proteção e Defesa do Consumidor.

Ressalte-se que apesar das bases legais dispostas nos incisos II a X dispensarem o consentimento do titular, restam resguardados seus direitos, conforme disposto no parágrafo 6º do artigo 7, especialmente no que diz respeito à informação, vide o disposto no artigo 9º. Assim, a dispensa do consentimento não afasta os deveres dos agentes de tratamento trazidos pela lei.

Diante exposto, conforme explanado, os dados pessoais sempre foram protegidos em legislações esparsas, contudo, nunca foram de fato reverenciados adequadamente como propriedade única de seu titular, o que possibilitou a coleta e o tratamento sem finalidade relevante para o cidadão, e, muitas vezes, sem qualquer consentimento.

A falta de orientação quanto a importância e o valor dos dados pessoais também impactaram o cenário, facilitando a prática abusiva de mercado. Tais fatos revelaram a importância de uma legislação específica quanto a proteção de dados, objetivando relacionar princípios, garantias, direitos e deveres a todos os envolvidos na coleta e no tratamento como um todo.

Importante destacar, que, em que pese haver a partir de agosto de 2020 uma legislação regulamentando o tema, o cidadão precisa ter ciência do valor de seus dados e da importância que possuem para o mercado. Para tanto, são importantes ações de conscientização e ampla divulgação da legislação, visando manter o cidadão informado.

"É de suma importância a compreensão de direitos e deveres, e o discernimento do que significa ceder os dados pessoais, e do prejuízo relacionado à sua exposição, viabilizando uma mudança de cultura no que se refere à propriedade e à cessão."

Essa conscientização vai permitir um nível diferenciado de atenção e maior critério quanto a disponibilização dos dados pessoais, realizando um empoderamento informacional. Possibilitará também que o cidadão se torne realmente dono de suas informações e de seus dados, especialmente nas ocasiões em que o consentimento é necessário, ocasionando que o aceite não seja algo meramente *pro forma*, ajustando o mercado para esse novo formato de tratamento de dados pessoais.

Ressalte-se que, a legislação seguiu um parâmetro internacional, tendo se inspirado na ***GDPR - General Data Protection Regulation***, permitindo que o Brasil se posicione em igualdade com os demais países que já possuem proteção de dados pessoais, favorecendo o comércio e as relações internacionais, fortalecendo a economia e a imagem do país.

Toda mudança de paradigma requer esforço. Para que haja resultado e que a legislação realmente seja adequadamente aplicada e amplamente observada é imprescindível que haja uma mudança de cultura, onde todos os envolvidos no processo de tratamento de dados pessoais se adequem à legislação e que seus titulares acompanhem atentamente as mudanças, cientes de suas implicações em caso de inobservância.

Ana Paula Canto de Lima

Advogada, palestrante, escritora e coordenadora de diversas obras jurídicas, professora, especialista em Direito da Internet, mestranda da UFRPE, fundadora do escritório Canto de Lima Advocacia. Membro fundador da Academia Brasileira de Ciências Criminais, onde preside a Comissão de Crimes Cibernéticos. Coordenadora do Núcleo de Direito e Tecnologia da ESA/PE, Assessora Jurídica da Corregedoria Seccional OAB/PE, CEO do curso Império Jurídico, redatora executiva da Revista Paradigma Jurídico e diretoria acadêmica da associação Law Talks.

Gabriela Rodrigues Sotero Caio

Bacharel em direito pela Universidade Católica de Pernambuco, advogada, pós-graduanda em Direito Digital pela FMP - Fundação Escola Superior do Ministério Público, membro da Comissão de Direito e Tecnologia da Informação da Ordem dos advogados de Pernambuco.

Manoela Gouveia Cabral de Vasconcelos

Advogada. Pós-graduada em Direito Público pela Estácio de Sá/CERS. Bacharela em Direito pela Universidade Federal de Pernambuco (UFPE). Membro da Comissão de Direito da Tecnologia e da Informação (CDTI) da OAB/PE. Orientadora do grupo de Privacidade e Proteção de Dados do grupo de extensão Discutindo Direito e Tecnologia (DDIT) da UFPE. Alumni do Insper no Curso de Direito Digital. Cofundadora do Coletivo Essa Moça Tá Diferente. Dedica sua pesquisa à área de privacidade e proteção de dados.

Maria Beatriz Saboya Barbosa

Advogada, Bacharela em Direito pela Universidade Federal de Pernambuco, pós-graduada pela Universidade Anhanguera-Uniderp e atualmente atendendo ao curso de Lei Geral de Proteção de Dados do Instituto de Tecnologia e Sociedade – ITS Rio. Membro da Comissão de Direito da Tecnologia e da Informação da OAB/PE. Pesquisa e produção de conteúdo na área de Privacidade e Proteção de Dados. Cofundadora do Coletivo Essa Moça Tá Diferente.

Raquel Corrêa de Melo

Advogada, Professora Universitária, Especialista em Direito Público, Doutoranda em Direito Penal pela Universidad de Buenos Aires - UBA, Membro da Associação Nacional de Advogados Criminalistas - ANACRIM, Membro da Comissão de Direito da Tecnologia e da Informação - CDTI da OAB-PE, Proprietária do escritório Corrêa & Melo advocacia e consultoria jurídica.

Yanne Holanda

Graduanda em Direito pela Faculdade de Direito do Recife - UFPE, cofundadora do Coletivo Essa Moça Ta Diferente e codiretora do DDIT – UFPE. Membro da Comissão de Direito e Tecnologia da Informação- OAB/ PE.

Referências

- Cf. NASCIMENTO, Rodrigo. **O que, de fato, é Internet das Coisas e que revolução ela pode trazer?** Computerworld, 12 mar. 2015. Disponível em: http://computerworld.com.br/negocios/2015/03/12/o-que-de-fato-e-Internet-das-coisas-e-que-revolucao-ela-pode-trazer. Acesso em: 14 agosto 2019.
- SANTOS, Maike Wile dos. **O Big Data somos nós: a humanidade de nossos dados.** Jota, 16 mar. 2017. Disponível em: https://jota.info/colunas/agenda-da-privacidade-e-da-protecao-de-dados/o-big-data-somos-nos-a-humanidade-de-nossos-dados-16032017. Acesso em: 25 agosto de 2019.
- MALDONADO, Viviane Nóbrega. BLUM, Renato Opice, coordenadores. **LGPD: Lei Geral de Proteção de Dados comentada.** São Paulo: Thomson Reuters Brasil, 2019.

- BRASIL. **Constituição da República Federativa Brasileira de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 14 de agosto de 2019.
- BRASIL. **Código de Defesa do Consumidor.** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 13 de agosto de 2019
- BRASIL. **Marco Civil da Internet.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acessado em: 13 de agosto.
- BRASIL. **Lei Geral de Proteção de Dados.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acessado em: 16 de agosto de 2019.
- UNIÃO EUROPEIA. **Regulamento Geral da União Europeia**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex %3A32016R0679. Acessado em: 16 de agosto de 2019.

Capítulo 4

Compartilhamento de dados pelo poder público para entidades privadas

Amália Câmara
Amanda Lima
Andreza Santiago
Camila Vilela
Clarice Cardim
Jéssica Mendonça
Leila Soares
Renata de Gois

A partir do seu nascimento, suas informações pessoais passam a compor várias bases de dados do setor público. Logo na maternidade, você passa a constar em estatísticas de taxas de natalidade, de população e das enfermidades. Não só. A Certidão de Nascimento emitida no Cartório é apenas um dos primeiros contatos de seus **Dados pessoais** com sistemas de armazenamento de dados. Quase que imediatamente ao seu nascimento, você já tem um número de CPF e um número da Carteira do SUS, o que possibilita, entre outras coisas, o cruzamento de seus dados com os de seus genitores, irmãos, tios, avós, etc.

Ao crescer, você se registra em escolas, universidade pública, bancos; você obtém a carteira de identidade, a autorização para conduzir veículos, o título de eleitor; você paga impostos, frequenta médicos e hospitais públicos. E, ainda que isso signifique uma vida normal, existe uma grande coincidência que você deve se atentar: em todas as situações citadas você fornecerá dados pessoais que o requerente irá armazenar em algum **banco de dados** com finalidades que você pode desconhecer.

É fato que a coleta e armazenamento desses e de outros dados permite ao poder público a criação e efetivação de políticas públicas e a elaboração de serviços públicos mais eficientes e direcionados às necessidades dos cidadãos que contribuem com a qualidade de vida de seus usuários. Em princípio, esse **Tratamento de dados** não aparenta ser um problema, pois é esperado que o governo entregue serviços públicos de qualidade, beneficiando nossa vida, otimizando nosso tempo, fornecendo uma saúde pública de qualidade, melhorando a educação e a segurança.

Mas então, qual o problema do tratamento de dados pessoais pelo poder público?

Uma vez que nossos dados sejam utilizados para alcançar a **finalidade pública**, perseguindo o interesse público, objetivando a execução de suas competências legais - desde que de forma transparente ao cidadão e que tenha uma pessoa encarregada para supervisionar esse tratamento -, é possível, viável e muito interessante para população que se realize o tratamento, visto que é com esses dados que o poder público pode contribuir com melhorias e prover políticas públicas interessantes a todos.

Diante de tanto valor que esses dados possuem, a situação preocupante reside na possibilidade de que eles podem ser compartilhados e utilizados de forma arbitrária ou com desvio de finalidade, gerando um proveito econômico pelo setor público, com o risco de violação de **Privacidade** dos cidadãos.

O setor público detém a maior base de dados dos cidadãos e isso gera preocupações, pois essa base em mãos erradas ou utilizada com objetivos escusos, obscuros, incertos, pode gerar diversos inconvenientes à população, levando-a a questionar o papel do Estado na concretização de seu papel institucional de proteção da sociedade.

Imagine se o setor público fornecesse todos os seus dados de contato para empresas de telemarketing e a partir daí você passasse a receber inúmeras propostas de serviços e produtos, dia e noite. Observa-se que costumeiramente, ao se aposentar (ou até mesmo antes de se ter conhecimento do deferimento da aposentadoria), o cidadão começa a receber propostas de empréstimos por empresas que trabalham com crédito consignado. Essas informações são obtidas de forma ilegal, mas já demonstram o valor de dados que o Poder Público possui e ressaltam a necessidade de controle efetivo quanto ao seu compartilhamento com entidades privadas.

"Essa base em mãos erradas ou utilizada com objetivos escusos, obscuros, incertos, pode gerar diversos inconvenientes à população"

A título de exemplo. Entretanto, na região metropolitana do Recife casos diários como bloqueamento do cartão de passe livre nos VEMs parecem ser algo inofensivo e comum, entretanto, as câmeras instaladas pela CTTU dentro dos ônibus fazem esse trabalho de monitoramento constante, em que, quando captura outro indivíduo utilizando este cartão de benefício, cancela-o automaticamente. A ação do usuário do transporte público, em si, vai de encontro aos termos de anuência contratual, todavia, torna-se evidente que o método utilizado afeta não somente aquele grupo específico, mas sim, que somos monitorados o tempo inteiro.

Possuímos tantos dados em mãos do setor público, que é extremamente importante entender como eles serão tratados e com quem será compartilhado, afinal, em tempos modernos onde os dados são a nova ***commodity***, o interesse das empresas privadas em obtê-los representa o novo modelo de negócios que movimenta dezenas de milhões de dólares todos os anos.

Todavia não é porque o setor público possui prerrogativas de coletar, manter e tratar nossos dados, que essa permissão é irrestrita e para qualquer finalidade. Por isso, a ***Lei Geral de Proteção de Dados Pessoais*** também prevê sua aplicação para o tratamento de dados pessoais por pessoa jurídica de direito público, devendo ser observada pela União, Estados, Distrito Federal e Municípios.

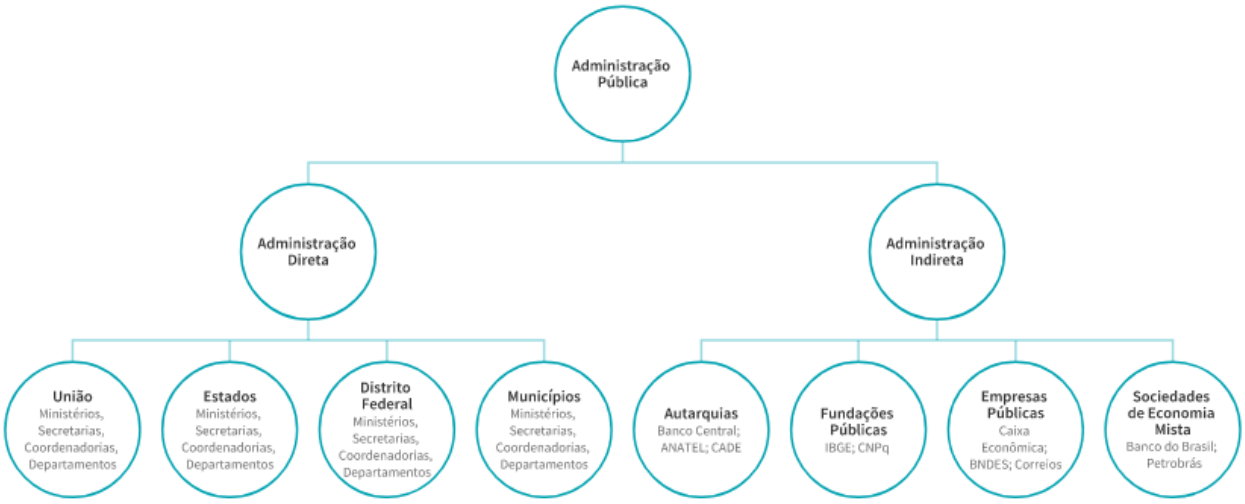
É importante lembrar também que o Governo não teria a capacidade de processamento para todos os dados e todas as pessoas, na sua atual conjuntura. Dessa forma, necessitar-se-ia de um intermediário (um operador - empresas terceirizadas) para regulamentar essas informações. Contudo, existem **Dados sensíveis** que só podem ser tratados pelo Estado, como os dados médicos, e daí que surge a complicação: como irá ser feita essa regulamentação?

"Entender quem é o setor público é essencial para compreender a amplitude da aplicação da LGPD"

Para regulamentar as situações de tratamento de dados pessoais, a LGPD além de explicar como empresas privadas devem realizar o tratamento de dados pessoais, traz também normas diferenciadas e mais flexíveis quando o dado é tratado pelo setor público, a depender de que tipo de organização é, quem vai tratar os dados pessoais e com qual finalidade. Assim, dispõe no Capítulo II o tratamento para dados pessoais de forma geral; e, no Capítulo IV, traz regras específicas para o tratamento de dados pessoais pelo setor público.

Entender quem é o setor público é essencial para compreender a amplitude da aplicação da LGPD neste contexto. Porém, é necessário recorrer ao **Direito Administrativo** para que se consiga absorver as definições dos diferentes tipos de entes e entidades para saber que parte da LGPD se aplica a cada caso específico.

De forma sucinta, a administração pública pode exercer suas atividades diretamente ou por meio de Órgãos, mas também pode criar uma pessoa jurídica para exercer determinadas atividades. Quando os Entes (União, Estados, Municípios, DF) exercem por conta própria os serviços, tem-se a **Administração Direta**. Quando ele cria e direciona para outra pessoa jurídica (Autarquia, Fundações Públicas, Sociedades de Economia Mista, Empresas Públicas), tem-se a **Administração Indireta**.



A Administração Pública pode agir basicamente em duas perspectivas: uma voltada para a finalidade pública, perseguindo o interesse público com o objetivo de executar as competências legais ou cumprir atribuições legais do serviço público; e no caso específico de Empresas Públicas e Sociedades de Economia mista que atuam em regime de concorrência, ou seja, visam ao lucro e concorrem diretamente com o mercado privado (ex: bancos públicos).

Nesse sentido, é necessário saber na situação específica qual o interesse do ente/entidade, se público ou concorrencial e, a partir daí, pode-se direcionar para as regras do Capítulo adequado (II ou IV). Ou seja, existirão **Empresas Públicas** e **Sociedades de Economia Mista** que ora atuam com finalidade pública, ora atuam com atividades concorrenciais; nesses casos haverá uma aplicação híbrida da LGPD, mesclando - para mesma entidade - duas formas de aplicação que deverão ser consideradas no caso concreto.

Quando for para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas

em contratos, convênios ou instrumentos congêneres, deverão ser observadas as disposições do Capítulo IV da LGPD (artigo 7º, III) e esta é uma das 10 hipóteses de tratamento de dados permitida pela LGPD.

Quando não houver a finalidade pública, para que se possa tratar os dados pessoais, a Empresa Pública ou **Sociedade de Economia Mista**, deverá se adequar a outras possibilidades de tratamento de dados e ainda se submeter a todas as regras aplicadas a pessoas jurídicas de direito privado.

Conforme dito anteriormente, durante nossa vida precisamos realizar inúmeros registros, cadastros e prestar informações, essa base de dados que o governo possui é alimentada com nosso nome, endereço, idade, **dados biométricos**, dados de saúde, dados sobre a vida financeira, dados educacionais, dados trabalhistas, dados de processos judiciais.

Em regra, o setor público pode tratar todos os dados que tem sob sua guarda, mas desde que obedeça à **finalidade** a que foi proposto, sem extrapolar os limites estabelecidos na hora da coleta ou para o atingimento do interesse público.

Além disso, vale lembrar que, para a LGPD, tratamento engloba muitos significados e, na forma como conceitua, o uso compartilhado de dados não está incluído como uma das possibilidades. Para se ter ideia, o tratamento envolve "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", conforme bem representado pela nuvem textual a seguir:

Como exemplo de tratamento de dados pelo poder público, é importante mencionar os recentíssimos decretos nº 10.046 e nº 10.047, publicados em outubro de 2019, que instituíram o Cadastro de Base do Cidadão e do Observatório de Previdência e Informações no âmbito do Cadastro Nacional de Informações Sociais (CNIS). Tais iniciativas consistem na criação e regulamentação de diretrizes para o **Compartilhamento de dados** entre a administração pública federal direta, autárquica, fundacional, os demais poderes da União, bem como, em alguns casos, com a iniciativa privada.

A China já utiliza um sistema similar na forma de *score* de crédito pessoal, o chamado Crédito Social[4]. Esse sistema pontua a população a partir do pagamento de suas compras. Também chamado de SPC totalitário pelo O Globo, poderá dar acesso a descontos em hotéis, alugueis de carros e obtenção mais rápida de vistos para aqueles que tiverem pontuações altas, no entanto, os que possuírem uma ficha "suja" não poderão inscrever seus filhos em escolas privadas, ter contratos com o Governo e nem seguir carreira militar.

[4] **BBC, (2017).** O plano chinês para monitorar – e premiar – o comportamento de seus cidadãos. Disponível em https://www.bbc.com/portuguese/internacional-42033007

O Cadastro Nacional de Informações Sociais (CNIS) será gerido pela Secretaria Especial de Previdência e Trabalho do Ministério da Economia e poderá compartilhar informações entre entidades públicas e privadas para fomentar a produção acadêmica e científica sobre estudos sociais, incentivar o compartilhamento de experiências, auxiliar os órgãos relacionados a políticas sociais e evitar fraudes (Artigo 4º - Decreto nº 10.047).

O CNIS será responsável pela unificação de 51 bases de dados relacionadas ao desenvolvimento social. Os dados constantes no CNIS poderão ser disponibilizados para a iniciativa privada desde que tal compartilhamento respeite as hipóteses de tratamento de dados pelo poder público, conforme delimitado pela LGPD. No caso, é fundamental que o compartilhamento possua como finalidade a execução dos objetivos previstos no próprio decreto, ou seja, fomentar a pesquisa e a troca de experiência que agregam o desenvolvimento social.

"existe a previsão de afastamento da exigência da anonimização desde que seja proferido Ato devidamente fundamentado"

Ainda é importante frisar que a regra do compartilhamento entre pessoas públicas e privadas, nos termos do decreto nº 10.047, é de que as informações compartilhadas possuam apenas ***Dados anonimizados*** , ou seja, de maneira que não seja possível identificar o titular do dado compartilhado. Porém, existe a previsão de afastamento da exigência da Anonimização desde que seja proferido Ato devidamente fundamentado para tal, sendo o mesmo de competência da Secretaria Especial de Previdência e Trabalho do Ministério da Economia (Artigo 4º, §1º Decreto Lei nº 10.047).

O decreto nº 10.046, publicado em outubro de 2019, instituiu do Cadastro de Base do Cidadão com o objetivo de otimizar e simplificar a oferta de serviços públicos por meio da criação de uma interface simples, que deverá ser capaz de unificar informações relevantes sobre o cidadão de forma direta.

O Cadastro Base do Cidadão, incialmente, irá preencher sua base de dados com "dados biográficos", ou seja, dados de pessoa natural relativos aos fatos da

sua vida, tais como nome civil ou social, data de nascimento, filiação, naturalidade, nacionalidade, sexo, estado civil, grupo familiar, endereço e vínculos empregatícios e, posteriormente, a base de dados poderá ser acrescida por demais dados que vinculem o titular aos seus dados biográficos.

Tal Cadastro será gerido pelo recém instituído Comitê Central de Governança de Dados que será o responsável por toda a análise de risco do compartilhamento de dados, conforme previsto no Artigo 21 do Decreto nº 10.046, que contará apenas com agentes públicos, não haverá participação popular direta na gestão dos dados - não obstante a população ser a titular dos dados que serão tratados. Ante tal situação, é preciso atenção redobrada do Estado a fim de evitar incidentes de segurança.

Os cadastros em desenvolvimento se tornarão importantes bases de dados, pois conterão dados pessoais e dados pessoais sensíveis dos cidadãos sob o fundamento de execução de políticas públicas. Para que tal fundamento se mantenha legítimo, é de suma importância que os gestores e comitês designados para a administração estejam conscientes da necessidade de adequação de todos os seus procedimentos com a lei geral de proteção de dados.

"É de suma importância que os gestores e comitês designados para a administração estejam conscientes da necessidade de adequação de todos os seus procedimentos com a lei geral de proteção de dados"

Ou seja, caso deseje compartilhar os dados constantes na sua base, o setor público deve observar regras específicas a respeito do tema, mas que, em linhas gerais, devem atender à finalidade específica de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no Artigo 6º (finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência segurança, prevenção, não discriminação, responsabilização e prestação de contas).

Destacamos ainda que as normas para a governança no compartilhamento de dados dentro da Administração Pública Federal, como

explica Danilo Doneda[5], vai na contramão do que vemos em países como Reino Unido, Austrália, Canadá e Finlândia, de ter um nível de uso de dados com certa interoperabilidade entre eles, feito dentro de um ordenamento de transparência, com instrumentos que dão controle ao cidadão de como o dado dele é usado[6].

Há vários questionamentos e posicionamentos sobre o mencionado Decreto, sobretudo porque o disposto nele é um grande desafio ao debate à privacidade, especialmente considerando que muitos dos dados fornecidos pelo cidadão ao governo não o são de forma voluntária, mas obrigatória. E que, agora, os dados que serão coletados e compartilhados entre os órgãos de governo vão muito além dos chamados dados pessoais, como bem explica Carlos Affonso[7].

Assim, é importante entender o que a LGPD define como uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados (Artigo 5º, XVI).

Além disso, em regra, é vedado pelo poder público transferir dados a que tenha acesso em sua base de dados para entidades privadas. Mas existem situações que isso pode ocorrer. São elas:

---

[5] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.
[6] LUCA, Cristina de. **Decreto de Bolsonaro aproxima uso de nossos dados a países como China**. Disponível em: <https://porta23.blogosfera.uol.com.br/2019/10/13/governo-tem-nossos-dados-mas-nao-deve-trata-los-como-se-fosse-o-dono-deles/?cmpid=copiaecola>. Acesso em 28 de out. 2019.
[7] AFFONSO, Carlos. **Por que é um risco um cadastro com rosto, RG e até nosso modo de andar**. Blog Tecfront. <https://porta23.blogosfera.uol.com.br/2019/10/13/governo-tem-nossos-dados-mas-nao-deve-trata-los-como-se-fosse-o-dono-deles/?cmpid=copiaecola> Acesso em 28 de out. 2019.

(i) em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente, para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (***Lei de Acesso à Informação***);
(ii) diante da designação de encarregado legal para o tratamento de dados pessoais;
(iii) quando houver previsão legal ou quando a transferência for respaldada em contratos, convênios ou instrumentos congêneres.
Neste ponto, destaca-se a propositura de requisitos alternativos, ao passo que tanto a previsão legal, quanto a disposição contratual viabilizam a transferência de dados. Tal redação legislativa atendeu à sugestão do Ministério da Fazenda que ressaltou que a previsão cumulativa inviabilizaria a estruturação da máquina pública que, por sua vez, detém muitos dados articulados em atos infraconstitucionais;
(iv) com objetivo de prevenir fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular de dados. Trata-se de hipótese com amplo alcance e com contornos pouco definidos, o que, de logo, coloca em alerta a apresentação de justificativa prudente acerca das razões públicas de transferências de dados, para que sob o argumento de protegê-los, não se possibilite a transferência indiscriminada de informações;
(v) quando os dados forem acessíveis publicamente.

"o Poder Público exerce sua função institucional de zelar pela uniformidade da interpretação e implementação da lei"

Ademais, ainda, no tocante a transferências de dados entre setor público e privado, importa destacar a aplicação da regra geral, a qual exige o consentimento do titular, diante da disponibilização de dados, sendo esta determinação excetuada em três possibilidades: (i) nas hipóteses de dispensa de consentimento previstas na LGPD; (ii) nos casos de uso compartilhado de dados, em que será dada publicidade às informações sobre os procedimentos utilizados e (iii) nas demais exceções ditadas na LGPD com relação ao Poder Público.

Assim, é de se notar que o Poder Público não passará ao largo das determinações exaradas pela Lei de Proteção de Dados. A **Autoridade Nacional**, também, cumprirá seu papel fiscalizando o Poder Público e, ao observar que houve infração da LGPD, poderá informar quais medidas devem ser adotadas

para que seja cessada a violação da lei. Sendo necessário dizer, ainda, que a ANPD poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais. E, de igual forma, poderá solicitar a agentes do Poder Público a publicação de Relatórios de Impacto à Proteção de Dados Pessoais (RIPDP) e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

Conclui-se, sobretudo, que o Poder Público exerce sua função institucional de zelar pela uniformidade da interpretação e implementação da lei diante das questões que proverão no contexto da aplicação da LGPD.

Amália Câmara
Professora de direito da Universidade de Pernambuco. Doutora em Direito pela UFPE. Doutora em Ciências Políticas pela UFPE e Coordenadora da Liga de Direito Digital.

Amanda Arruda Lima
Graduanda em Direito pela Universidade Católica de Pernambuco; membro da Comissão de Direito e Tecnologia da Informação - OAB/PE.

Andreza Felipe Santiago
Graduanda em Direito pela Faculdade Imaculada Conceição do Recife; estagiária; membro da Comissão de Direito e Tecnologia da Informação OAB/PE"

Camila Maria de Moura Vilela
Advogada e professora, mestranda em Direito Intelectual pela Universidade de Lisboa (FDL), participação especial no Curso de Pós-graduação em Direito Intelectual (APDI), pós-graduada em Direito Público (ASCES-UNITA), membro associada à Associação Portuguesa de Direito Intelectual (APDI), cofundadora do Legal Hackers Lisboa.

Clarice Cardim
Advogada, designer, pós-graduanda em Direito Digital (Damásio Educacional), membro da Comissão de Direito e Tecnologia da Informação OAB-PE e membro da Comissão de Direito das Startups OAB-PE.

Jéssica M. Mendonça de Lima Melo
Advogada, Mestranda em Propriedade Intelectual e Transferência de Tecnologia pela Universidade Federal de Pernambuco, membro da Comissão de direito da tecnologia e da informação.

Leila Farias Soares
Graduanda em Direito pela FICR- Faculdade Imaculada Conceição do Recife; Monitora das disciplinas: Direito Penal I; Direito Penal II; Direito Penal III e Direito Civil IV, respectivamente em 2017, 2018 e 2019; Aprovada no Projeto de Iniciação Científica da FICR em Criminologia (2018); Estagiária da Procuradoria Geral do Município - CRA (agosto de 2018 a setembro de 2019); Membro da Comissão de Direito da Tecnologia da Informação- OAB/PE.

Maria Renata Gois

Graduanda em direito pela Universidade de Pernambuco, pesquisadora do grupo Smart Cities da Universidade de Pernambuco, PIBicanda em Inteligência Artificial, membro colaborador da comissão de direito e tecnologia da informação da OAB/PE.

Referências

- AFFONSO, Carlos. **Por que é um risco um cadastro com rosto, RG e até nosso modo de andar.** Blog Tecfront. Disponível em: <https://porta23.blogosfera.uol.com.br/2019/10/13/governo-tem-nossos-dados-mas-nao-deve-trata-los-como-se-fosse-o-dono-deles/?cmpid= copiaecola> Acesso em 28 de out. 2019.
- BIONI, Bruno Ricardo. **Proteção de dados pessoais: A função e os limites do consentimento.** Forense, 2019.
- BBC, (2017). **O plano chinês para monitorar – e premiar – o comportamento de seus cidadãos**. Disponível em: <https://www.bbc.com/portuguese/internacional-42033007> Acesso em 28 de out. 2019
- BRASIL. Presidência da República. Decreto 10.046 de 9 de outubro de 2019. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm Acesso em: 27 out. 2019
- BRASIL. Presidência da República. **Decreto 10.047** de 9 de outubro de 2019. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10047.htm Acesso em: 27 out. 2019
- BRASIL. Presidência da República. **Lei nº 13.709**, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGDPD).** (Redação Dada pela Lei nº 13.853, de 2019). Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 30 nov. 2019
- BRASIL. Presidência da República. **Lei nº 12.527**, de 18 de novembro de 2011. **Lei de Acesso à Informação.** Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 27 out. 2019
- **CTTU. Central de Operação de Trânsito**. Disponível em: <http://cttu.recife.pe.gov.br/central-de-operacao-e-transito Acesso em 28 de out. 2019
- DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.
- LUCA, Cristina de. **Decreto de Bolsonaro aproxima uso de nossos dados a países como China**. Disponível em: <https://porta23.blogosfera.uol.com.br/2019/10/13/governo-tem-nossos-dados-mas-nao-deve-trata-los-como-se-fosse-o-dono-deles/?cmpid=copiaecola>. Acesso em 28 de out. 2019.
- MENDES, Laura Schertel. **Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo**. 2008.
- **O direito fundamental à proteção de dados pessoais**. Revista de Direito do Consumidor, v. 79, p. 45-81, 2011.
- MALDONADO, Viviane Nóbrega; BLUM, Renato Opice; BORELLI, Alessandra. **Comentários ao GDPR: regulamento geral de proteção de dados da União Europeia**. 2018.
- **LGPD: Lei geral de proteção de dados: comentada**. 2019.
- DIAS, Tatiana. **Aqui estão todas as suas informações que o governo vai reunir numa megabase de vigilância**. The Intercept Brasil, 15 out. 2019. <https://theintercept.com/2019/10/15/governo-ferramenta-vigilancia/> Acesso em: 28 out. 2019.
- ORWELL, George. **1984**. 1ª Edição. São Paulo: Editora Companhia das Letras, 2009.

Capítulo 5

Dados da saúde: a possibilidade de compartilhamento para fins de prestação suplementar de serviços e assistência

Camila Andrade Silveira Lima
Flávia de Carvalho Silva
Gabriela Santos Stamford Gaspar
Pedro Ivo de Oliveira Rodrigues

Com o grande acúmulo de dados hospitalares, grandes também são os desafios para a aplicação, adoção, análise e manuseio deles. É por essa razão que as habilidades e competências digitais entre profissionais e gestores de saúde devem ser desenvolvidas, uma vez que atualmente há o uso massivo de prontuários médicos eletrônicos, tecnologia móvel em saúde (***m-Saúde***), dispositivos vestíveis (***wearables***), serviços de telessaúde, teleconsultas, telemedicina, entre outros[8].

É neste cenário que surge a preocupação com o **Tratamento** dos **Dados sensíveis** pelos estabelecimentos, principalmente os que dizem respeito a informações médicas, vida sexual e dados genéticos da pessoa natural, e de como tais informações podem ajudar na implementação de políticas públicas, na qualidade dos serviços, no tratamento de doenças e na manutenção/viabilização da cobertura universal da saúde com o auxílio das **TIC**.

Na área da saúde, já existem orientações práticas e dispositivos legais em vigor que permitem instituições atuantes neste segmento garantirem a **Privacidade** de dados e informações nas suas operações como o Código de Ética Médica[9] e

[8] **Medição da saúde digital**: recomendações metodológicas e estudos de caso [livro eletrônico] / Organização Pan-Americana da Saúde, Núcleo de Informação e Coordenação do Ponto BR; Ana Laura Martínez, David Novillo Ortiz & Fabio Senne (coords.). -- São Paulo: Comitê Gestor da Internet no Brasil, 2019. 2.700 Kb ; PDF. p 12.

[9] Disponível em: <https://portal.cfm.org.br/images/stories/biblioteca/codigo%20de%20etica%20medica.pdf> Acesso em 24 de jul de 2019.

a Resolução Nº1821/07 do Conselho Federal de Medicina. No entanto, a Lei Geral de Proteção de Dados (nº 13.709) aparece para esclarecer e ampliar o entendimento quanto a alguns pontos.

Conforme o artigo 5º da Lei Geral de Proteção de Dados, dado pessoal é toda informação relacionada a uma pessoa natural, seja ela identificada ou identificável. Já dado pessoal sensível é toda informação sobre "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

"dado pessoal é toda informação relacionada a uma pessoa natural, seja ela identificada ou identificável"

Os dados sensíveis possuem informações que podem gerar grande exposição na vida social e profissional do seu titular. Sendo assim, para respeitar a privacidade e garantir que eles não sejam utilizados contra os próprios titulares gerando restrições ao acesso de serviços e bens, o tratamento desses dados deve ser feito com muito rigor e cautela à luz do artigo 11 da ***Lei Geral de Proteção de Dados Pessoais* (LGPD)**. Se não existir um tratamento diferenciado, dados importantes como biometria, imagens faciais, impressões digitais e dados físicos e psicológicos podem gerar grande risco de discriminação por parte dos planos de saúde, por exemplo.

Ao analisar o texto da lei, nota-se que existe um grande paralelismo entre os artigos 9 e 11 da LGPD ficando claro que todos os cuidados tomados no tratamento dos **Dados pessoais** também devem ser aplicados aos dados sensíveis. Uma importante diferença é que, para que possam ser tratados, os dados sensíveis precisam ser expressamente autorizados para um determinado fim pelo titular e caso a finalidade do tratamento seja modificada será necessária uma nova autorização (Artigo 11, I). No entanto, a legislação também traz um **Rol taxativo** de outras hipóteses em que pode ocorrer esse tratamento, sem que haja o consentimento do titular, como nos casos em que for indispensável para tutela da saúde, exclusivamente em procedimento realizado por profissionais ou serviços de saúde ou autoridade sanitária (Artigo 11, II, "f").

No setor público, como bem explicado no capítulo anterior, a utilização de banco de dados pessoais é de extrema importância, uma vez que é necessário para efetivar suas políticas públicas em diversos setores, sobretudo na saúde pública. Diante disso, para que o tratamento desses dados pelo Poder Público ocorra em conformidade com a lei, é preciso que medidas de segurança, técnicas e administrativas sejam adotadas. Caso esteja vigorando a permissão de tratamento dos dados sensíveis, é importante também que o Poder Público se atente ao fato de que este tratamento deve ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público (Artigo 23, caput).

"para que o tratamento desses dados pelo Poder Público ocorra em conformidade com a lei, é preciso que medidas de segurança, técnicas e administrativas sejam adotadas"

Diante disso, em consonância com a LGPD e com o princípio da publicidade, é necessário que sejam fornecidas informações claras e atualizadas sobre a finalidade, os procedimentos e as práticas utilizadas no tratamento de dados, em veículos de fácil acesso, preferencialmente em sites eletrônicos (Artigo 23, I). Caso os dados necessitem ser usados em uso compartilhado, eles devem ser mantidos em formato interoperável e estruturados (Artigo 25).

Um tema bastante discutido é a possibilidade de compartilhamento dos dados de saúde para fins de prestação suplementar, ou seja, operação de planos e seguros privados de assistência médica à saúde. Nesse sentido, é importante evidenciar a lei 13.853/19, que surgiu através da MP 869/18 e trouxe algumas mudanças acerca do tratamento dos dados:

- Ampliou as hipóteses relacionadas à comunicação e compartilhamento dos dados, abrangendo os que são relacionados à assistência farmacêutica e serviços auxiliares de diagnose e terapia, bem como as solicitações de

portabilidade pelo titular ou para transações resultantes do uso e da prestação de serviços financeiros e administrativos;

- Vedou a utilização dos dados pelas operadoras de planos de saúde com a finalidade de seleção de riscos ou contratação/exclusão de beneficiários;
- Nos casos de **Compartilhamento de dados** que tenham sido corrigidos, eliminados, bloqueados ou **anonimizados**, passou a existir a possibilidade de dispensar a comunicação entre o titular e o agente de tratamento caso ela seja considerada impossível ou demonstre necessidade de um esforço desproporcional;
- Estabeleceu, para as entidades privadas, condições de existência para o compartilhamento de dados pessoais de com bases nos órgãos do governo.

Antes da Lei 13.853 de 2019, era permitida a comunicação ou o uso compartilhado entre **Controlador de Dados** pessoais sensíveis referentes à saúde nas hipóteses de o compartilhamento ser necessário para a adequada prestação de serviços de saúde suplementar. Entretanto, foi constatado que essa permissão poderia ocasionar aumentos abusivos, negativas de tratamento ou de adesão e **Algoritmos** que causem a discriminação por parte dos planos de saúde, uma vez que o termo "adequada prestação" foi considerado impreciso. Diante disso, a versão atual da lei veda expressamente a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas seguintes hipóteses:

- Para a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados;
- Para permitir a portabilidade de dados quando solicitada pelo titular;
- Para permitir as transações financeiras e administrativas resultantes do uso e da prestação dos serviços da saúde.

Sendo estritamente proibido, mesmo que haja a necessidade do compartilhamento dos dados, que as operadoras de planos privados de assistência à saúde realizem o tratamento de dados de saúde para a prática de

seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.

Como já foi exposto, o **Vazamento de dados** médicos de uma pessoa natural traz enormes constrangimentos, prejuízos, pode acarretar a seleção de clientes pelos planos de saúde e negativa de serviços com base no histórico médico de quem teve os dados sigilosos expostos, ou ainda ser utilizados por cibercriminosos para o cometimento de diversos ilícitos.

Por essa razão, a LGPD em seu artigo 38 prevê que a Autoridade Nacional, objeto de estudo do nosso último capítulo, poderá elaborar relatório de impacto à proteção de dados pessoais, incluindo os dados sensíveis, referente a suas operações de tratamento, que deverá conter, no mínimo, "a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de riscos adotados". Acrescente-se que, em razão da necessidade de se adotar medidas de segurança, técnicas e administrativas, a Autoridade Nacional poderá impor padrões técnicos mínimos, dependendo da natureza das informações, das características específicas do tratamento e do estado atual da tecnologia. Ocorrendo um incidente, ela ainda pode determinar a adoção de providências, tais como a ampla divulgação do fato em meios de comunicação; e medidas para reverter ou mitigar os efeitos do vazamento.

"A Autoridade Nacional poderá impor padrões técnicos mínimos, dependendo da natureza das informações, das características específicas do tratamento e do estado atual da tecnologia"

Válido, ainda, ressaltar que todas as empresas envolvidas respondem solidariamente pelos danos patrimoniais, morais individuais e coletivos, tal como a violação de legislação (dever de reparação), caso se comprove que estavam diretamente envolvidas no tratamento dos dados que gerou o incidente, no tocante às credenciais de acesso, a menos que provem que não houve violação

à legislação de proteção de dados ou que os danos decorrentes foram culpa exclusivamente de terceiro (Artigo 43, incisos II e III).

Ademais, quanto às sanções (sem prejuízo da aplicação de sanções administrativas, civis ou penais definidas em legislação específica), após o procedimento administrativo que possibilite a oportunidade de ampla defesa, considerando a gravidade e a natureza das infrações, a boa-fé, a condição econômica, a reincidência, o grau do dano, a cooperação e a pronta adoção de medidas corretivas, entre outros critérios à luz do caso concreto, receberá da Autoridade Nacional, de forma gradativa, isolada ou cumulativa: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total de R$ 50.000.000,00 (cinquenta milhões de reais) por infração; IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; e VI - eliminação dos dados pessoais a que se refere a infração.

Portanto, é possível perceber que a LGPD causará profundos impactos na área da saúde pois esta atua diretamente com dados sensíveis, sobre os quais não se admite a hipótese de tratamento para atender interesses diversos daqueles que foram consentidos pelos titulares dos dados. Nesse sentido, é importante que aqueles que realizarão o tratamento, além de atender às normas já apresentadas, também garantam a aplicação de medidas de segurança aptas a proteger os dados pessoais sensíveis contra acessos não autorizados, e a implementação de processos e políticas internas que assegurem o cumprimento de normas e boas práticas relativas à proteção desses dados.

Camila Andrade Silveira Lima

Graduanda em Direito pela Universidade de Pernambuco. Estagiária da Defensoria Pública do Estado de Pernambuco. Membro colaboradora da Comissão de Direito e Tecnologia da Informação da OAB/PE. Participante dos cursos de Direito no Tempo dos Dados e Direito à privacidade na Transformação Digital pela César School. Pesquisadora do projeto de pesquisa "Formação Histórica do Controle de Constitucionalidade no Brasil".

Flávia de Carvalho Silva

Advogada formada pela UFPE. Técnica em Informática pelo IFAL. Pós-graduanda Lato Sensu em Direito Digital e Compliance. Palestrante. Pesquisadora na área de Direito & Internet e Direito Digital. Idealizadora do Grupo de estudos, pesquisa e extensão DDIT (Discutindo Direito Digital, Internet e Tecnologia) com atuação na Faculdade de Direito do Recife (UFPE).

Gabriela Santos Stamford Gaspar

Graduanda em Direito pela Universidade Católica de Pernambuco; Membro colaborativo da comissão de Direito e Tecnologia da Informação- OAB/PE

Pedro Ivo de Oliveira Rodrigues

Advogado, cientista da computação e professor, membro da Comissão de Direito da Tecnologia e da Informação da OAB/PE, membro da Comissão de Crimes Cibernéticos da Academia Brasileira de Ciências Criminais - ABCCRIM. Certificado Cisco Systems CCNA e CCAI, Especialista em Direito Público e Mestre em Gestão Empresarial.

Referências

- **Medição da saúde digital: recomendações metodológicas e estudos de caso** [livro eletrônico] / Organização Pan-Americana da Saúde, Núcleo de Informação e Coordenação do Ponto BR; Ana Laura Martínez, David Novillo Ortiz & Fabio Senne (coordenadores). -São Paulo: Comitê Gestor da Internet no Brasil, 2019. 2.700 Kb
- BRASIL, **Lei nº 13.709** (Lei Gera de Proteção de Dados), Artigo 5º, inciso II, Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acessado em: 24 de jul de 2019.
- **Código de Ética Médica**. Disponível em: <https://portal.cfm.org.br/images/stories/biblioteca/codigo%20de%20etica%20medica.pdf > Acessado em: 24 de jul de 2019.
- **Resolução CFM Nº 1.821/2007**. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2007/1821> Acessado em: 24 de julho de 2019.
- **Revista Exame.** Disponível em: <https://exame.abril.com.br/tecnologia/singapura-se-torna-alvo-cobicado-por-hackers-internacionais/>. Acessado em: 24 de julho de 2019.
- BRASIL. Presidência da República. **Lei nº 13.709**, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGDPD).** (Redação Dada pela Lei nº 13.853, de 2019). Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 30 nov. 2019
- BRASIL. Presidência da República. **Lei nº 13.853**, de 8 de julho de 2019. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/Lei/L13853.htm Acesso em: 25 out. 2019
- BRASIL. Presidência da República. **Medida Provisória nº 869**, de 27 de dezembro de 2018. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Mpv/mpv869.htm. Acesso em: 29 out. 2019

Capítulo 6

Proteção de dados em um cenário acadêmico

Josemário Júnior
Julyanne de Bulhões
Pedro Ivo de Oliveira Rodrigues

A LEI GERAL DE PROTEÇÃO DE DADOS E A HIPÓTESE DE TRATAMENTO DE DADOS PARA FINS ACADÊMICOS: CONCEITOS E COMENTÁRIOS INICIAIS.

Quantas vezes precisamos preencher formulários imensos, referente a inscrição em algum curso *on-line*, informando nossa filiação, estado civil e demais informações completamente dispensáveis à realização do curso em si, ou ainda, a emissão do certificado, por exemplo? Exato! Culturalmente, não nos questionamos o motivo de nossos dados serem coletados e sequer hesitamos em fornecê-los. Por essa razão, a **Lei Geral de Proteção de Dados (LGPD)** é um marco regulatório importante, sobretudo no papel do despertar social para a conscientização sobre os **Dados pessoais**.

Ocorre que, a LGPD prevê algumas hipóteses em que sua própria aplicação é dispensada ou é limitada, como, por exemplo, quando se fala em **Tratamento** de dados para fins exclusivamente acadêmicos. Nesse caso, não se aplicam todas as disposições da lei, mas, apenas naqueles referentes às bases legais para tratamento de dados pessoais e às limitações no tratamento de dados sensíveis – legalmente definidos como aqueles capazes de possuir maior teor discriminatório.

Contudo, os fins acadêmicos não foram mais bem enquadrados nas hipóteses legais, causando uma lacuna legislativa, que prescindirá futuramente de disciplina, seja pela atuação da **Agência Nacional de Proteção de Dados Pessoais - ANPD**, objeto de estudo do nosso último capítulo, seja pelo próprio comportamento da legislação no contexto social. Isso porque, atualmente,

quando diante de pesquisas acadêmicas não há como assegurar que o tratamento de dados pessoais se restringe tão somente ao escopo da pesquisa.

Assim, abordaremos o tratamento de dados para finalidade acadêmica, na tentativa de estabelecer alguns parâmetros para o entendimento da lei. Inclusive, com a discussão acerca de possíveis práticas para a efetiva proteção dos dados pessoais e, por óbvio, para a implementação da legislação prevista para entrar em vigor em agosto de 2020.

OS LIMITES E CONCEITOS PARA A PROTEÇÃO DOS DADOS PESSOAIS

A lei geral de proteção de dados (LGPD) determina limites ao tratamento dos dados. Sua aplicação se dá na forma prescrita pelo Artigo 3º, que visa delimitar a abrangência da lei. Assim, a LGPD determina que a legislação só é aplicável quando o tratamento de dados tiver o objetivo de ofertar ou fornecer bens ou serviços. Ou seja, é necessário que o tratamento de dados tenha uma finalidade econômica para que sejam aplicados os termos da lei.

No quesito territorialidade, a LGPD deverá ser aplicada sempre que houver o **tratamento de dados** de **pessoas naturais** independente da nacionalidade dessa pessoa, podendo ela ser brasileira ou estrangeira, desde que esteja em território brasileiro. Este mesmo diploma legal determina que a proteção aos dados deve ser observada independente do meio aplicado para realizar o tratamento, tal como meios físicos ou digitais.

Para a realização do tratamento dos **dados pessoais**, alguns requisitos legais devem ser cumpridos, como a atenção à boa-fé, a existência de finalidade, limites, prestação de contas, segurança, transparência a possibilidade de consulta por parte dos titulares dos dados. Neste contexto, fica evidente que a lei determina que o titular dos dados pessoais é o verdadeiro "dono" daquelas informações, possuindo, portanto, uma série de direitos sobre elas.

Desta maneira, a LGPD, em seu Artigo 7º, buscou coibir o uso indiscriminado de dados pessoais coletados pelos mais diversos meios, garantindo ao titular o direito de ser informado sobre como será realizado o tratamento de seus dados e para qual fim eles serão usados.

"A LGPD, em seu Artigo 7º, buscou coibir o uso indiscriminado de dados pessoais coletados pelos mais diversos meios, garantindo ao titular o direito de ser informado sobre como será realizado o tratamento de seus dados e para qual fim eles serão usados"

Diante de toda a proteção dada aos titulares de dados pessoais, esta mesma legislação definiu que alguns dados merecem um cuidado maior. Esses dados são classificados como dados pessoais sensíveis. Eles merecem uma atenção especial por parte do diploma legal porque a sua violação pode implicar em sérios riscos aos direitos e as liberdades fundamentais do titular dos dados. Esta atenção especial fica evidente ao se analisar o Artigo 11 da LGPD, o qual trata dos requisitos legais para a realização do tratamento de dados pessoais sensíveis. Um requisito que merece um destaque é o fornecimento do consentimento pelo titular dos dados para o seu tratamento. O consentimento pode ser relativizado em alguns casos conforme pontuado pelo Artigo 11 da LGPD.

TÉCNICAS PARA PROTEÇÃO DE DADOS EM UM CENÁRIO ACADÊMICO

O uso das tecnologias nas empresas permitiu velocidade no processamento das informações e uma maior capacidade para armazená-las. O uso dessa inovação na rotina das empresas possui um elevado custo, principalmente quando associado a segurança. Porém, pior é não destinar recursos para soluções que garantam ou ao menos elevem a segurança das informações processadas e armazenadas, pois a perda de dados pode gerar enormes prejuízos financeiros além de processos judiciais por danos morais e materiais. O uso de técnicas e ferramentas de proteção de dados é fundamental para a sobrevivência da instituição.

Em um ambiente acadêmico, as vulnerabilidades são inúmeras, tendo em vista a quantidade de pessoas com acesso a sistemas acadêmicos de notas e controle de frequência, além de sistema financeiro e de registros acadêmicos. Existem, contudo, técnicas que ajudam a proteger os dados nesse cenário, que elencamos a seguir:

Sistema de Antivírus

Os sistemas de antivírus são importantes em todas as empresas, pois por meio do uso de programas maliciosos, ***hackers*** podem obter ou destruir informações. Em um cenário acadêmico, onde alunos e professores utilizam computadores, próprios ou da instituição, em redes com ou sem fio, a vulnerabilidade aumenta, pois, o uso inadequado, muitas vezes desalinhado de políticas de segurança, pode ser uma porta de entrada para vírus e programas similares.

Firewall

Por meio de *firewall* (parede de fogo), a empresa se protege de diversos ataques, geralmente com maior eficácia contra-ataques vindo do mundo externo à empresa. Um *firewall* é composto por equipamentos e ***Software*** específicos com recursos para identificar quem está tentando acessar o que.

Sistemas de Backup

Os sistemas de *Backup* utilizam técnicas de cópias das informações para posterior verificação e acesso como forma de prevenção à perda de dados, seja por ataque intencional, descuido de funcionários ou desastres naturais. Um problema de sistemas de *backup* na prática é que muitos arquivos e informações de interesse da empresa não são postos nas cópias por negligência de funcionários.

Capacitação dos funcionários

A capacitação dos funcionários é a principal arma no combate ao **Vazamento de dados**, já que grande parte dos acessos indevidos ocorreu usando informações internas da empresa e isso, em muitos casos, é consequência de

atitudes descuidadas dos funcionários, que relutam em seguir as normas definidas na Política de Segurança Institucional, abrindo brechas para hackers.

Os dados são da pesquisa global em segurança da informação da *PricewaterhouseCoopers - PwC*, realizada em 2017 com 9.500 executivos em 75 setores de 122 países, onde os funcionários representam 30% dos incidentes com segurança nas empresas e ex-funcionários 26%. (*PricewaterhouseCoopers* Brasil, 2018). Isso acontece porque os funcionários não conseguem mensurar o real impacto da perda de informações para a vida da empresa, além da sensação constante de que a perda de dados não irá ocorrer consigo.

Política de Segurança da Informação

A Política de Segurança da Informação é a expectativa da empresa em relação à segurança, considerando o alinhamento com os seus objetivos de negócio, estratégias e cultura. Na implantação e manutenção das políticas de segurança, o apoio da direção é fundamental para que os funcionários e professores possam entender a importância de seguir as regras e os riscos de não o fazer. Além disso, conscientizar os alunos dos riscos e prejuízos em não seguir as regras de laboratórios ou de uso de dados acadêmicos, como em casos de pesquisas, é também crucial.

Sistemas de monitoramento

O sistema de monitoramento procura por vulnerabilidades que possam existir no ambiente empresarial. Não são muito comuns em ambientes acadêmicos, exceto monitoramento por vídeos (câmeras de segurança). A existência de vulnerabilidades é o cenário ideal para ameaças, tanto internas quanto externas, às empresas, e a prevenção através de diagnósticos em sistemas interconectados ajuda a identificar essas vulnerabilidades para então combatê-las, quando não as eliminar. A maior parte das vulnerabilidades nas empresas advém da falta de atenção com as normas de segurança que todos devem seguir.

Sistemas Acadêmicos

O acesso aos registros acadêmicos é feito por professores, alunos, coordenadores de cursos e secretarias escolares, ou suas equipes. A política de perfis de usuários é importante para controlar o limite de acesso aos sistemas. Um grande problema dentro desses perfis é o controle das alterações nos registros acadêmicos, que podem ser feitos pela Secretaria Acadêmica, porém sob o conhecimento e controle dos coordenadores de cursos e/ou professores, e vice-versa.

Josemário França de Sousa Junior

Engenheiro de Testes de Software do C.E.S.A.R., Professor do C.E.S.A.R. School, bacharel em Ciência da Computação, bacharel em Direito, membro da Comissão de Direito da Tecnologia e Informação da OAB/PE, Mestrando em Ciências da Computação no Centro de Informática da UFPE.

Julyanne Cristine de Bulhões da Silva Nascimento

Bacharel em direito pela UNICAP, advogada, pós-graduanda em Legal Tech pela PUC-Minas, membro da Comissão de Direito e Tecnologia da Informação e da Comissão de Propriedade Intelectual ambas da Ordem dos advogados de Pernambuco; Cofundadora do coletivo Essa Moça Tá Diferente.

Pedro Ivo de Oliveira Rodrigues

Advogado, cientista da computação e professor, membro da Comissão de Direito da Tecnologia e da Informação da OAB/PE, membro da Comissão de Crimes Cibernéticos da Academia Brasileira de Ciências Criminais - ABCCRIM. Certificado Cisco Systems CCNA e CCAI, Especialista em Direito Público e Mestre em Gestão Empresarial.

Referências

- ESTADÃO. **LGPD: entenda o que é a Lei Geral de Proteção de Dados Pessoais**. Disponível em: <https://politica.estadao.com.br/blogs/fausto-macedo/lgpd-entenda-o-que-e-a-lei-geral-de-protecao-de-dados-pessoais//>. Acesso em: 26 agosto 2019.
- PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: comentários à lei n. 13.709/2018 (LGPD)**. São Paulo: Saraiva Educação, 2018.
- SERPRO. **Serpro e LGPD: segurança e inovação**. Disponível em: <https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd/>. Acesso em: 26 agosto 2019.
- PricewaterhouseCoopers Brasil Ltda. **Global State of Information Security Survey 2018**. Disponível em: <https://www.pwc.com.br/pt/global-state-of-information-security-survey-2018.html>. Acesso em 28 de agosto de 2019.
- BRASIL. Presidência da República. **Lei nº 13.709**, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGDPD).** (Redação Dada pela Lei nº 13.853, de 2019). Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 30 nov. 2019

Capítulo 7

Direito de Revisão: automatizada?

André Ramiro
Barbara Santini
Genifer de Andrade
João Paulo Borba Maranhão
Tatiana Lucena
Thaís Aguiar

CONCEITO

De acordo com o **Fórum Econômico Mundial**, a sociedade hoje vive a quarta revolução tecnológica, marcada pela profunda interferência das tecnologias da informação e comunicação na maneira em que as pessoas vivem e entidades governamentais formulam estratégias políticas.

Tanto em termos qua'ntitativos quanto qualitativos, as informações geradas a todo tempo na Internet são úteis para diversos fins, como científicos e econômicos, através da ciência de dados. É por isso que termos como **Inteligência artificial** , **Algoritmos**, ***Big data*** e ***Machine Learning*** se tornaram tão populares ultimamente e dizem respeito a **Direitos fundamentais** e modelos de negócios - aqui, uma breve explicação.

Os algoritmos, por exemplo, não são novidade da computação: já há referências desde os matemáticos gregos, como o algoritmo euclidiano para encontrar o maior divisor comum entre dois números. Apesar da ampla literatura em computação e da questão matemática desafiadora de definir o conceito, os algoritmos podem ser compreendidos, grosso modo, como um conjunto de instruções tipicamente utilizado para resolver problemas. Dessa forma, qualquer tipo de passo a passo pode ser considerado um algoritmo.

Na era da sociedade da informação, os algoritmos ganham ainda mais importância por estarem no centro das operações realizadas por computadores. Eles são muito úteis para manipular quantidades enormes de dados - isto é, o *Big*

Data. As informações obtidas dependem, evidentemente, do objetivo que se estabelece, e hoje é muito comum que o "oceano de dados" disponível na Internet seja utilizado a favor de diversas finalidades, com destaque para a comercial.

Quanto mais dados disponíveis, mais frutífero o ambiente é para análises em ciência de dados. Isso contribui para a ascensão da inteligência artificial, que é quando máquinas ou "*agentes inteligentes*" interpretam corretamente dados externos e constroem a capacidade de adaptação flexível para executar tarefas. E, na mesma linha, o aprendizado por máquina ou *machine learning* utiliza dados para construir análises preditivas, identificação de padrões e tomadas de decisão com relativa independência de seres humanos.

NORMAS, LEIS E PRINCÍPIOS

A ***Lei Geral de Proteção de Dados Pessoais*** dispõe a respeito do **Tratamento** de **Dados pessoais** e tem como objetivo a proteção de direitos fundamentais dos **titulares** destes dados. Ela teve como principal inspiração a **General Data Protection Regulation** da União Europeia e ambas possuem diversos dispositivos com temática em comum. A LGPD foi sancionada em 14 de agosto de 2018, tendo inicialmente o período de ***Vacatio legis*** de 18 meses, posteriormente prolongado para 24 meses. O texto entrará em vigor no dia 16 de agosto de 2020 e trará regulações que buscam assegurar a segurança dos dados pessoais.

A LGPD trata da revisão automatizada em seu Artigo 20. Nele se estabelece que o titular dos dados tem direito a solicitar revisão de decisões que sejam tomadas com base apenas em **Tratamento automatizado**. Entre os dados em questão estão aqueles relacionados aos perfis pessoal, profissional, de consumo, de crédito ou outros aspectos da personalidade do titular.

Em seu § 1º também é estabelecido que as informações a respeito dos critérios e procedimentos utilizados no tratamento dos dados deverão ser fornecidas de forma clara e adequada após solicitação do titular, sendo preservados os segredos comerciais e industriais.

Caso as informações solicitadas não sejam fornecidas, nos termos do § 1º deste artigo, determina o § 2º que poderá ser realizada auditoria pela autoridade

nacional para verificar eventuais aspectos discriminatórios no tratamento dos dados.

A Lei 13.853/2019 incluiu no Artigo 20 o § 3º que dispunha que "A revisão de que trata o caput deste artigo deverá ser realizada por pessoa natural, conforme previsto em regulamentação da autoridade nacional, que levará em consideração a natureza e o porte da entidade ou o volume de operações de tratamento de dados". Porém o dispositivo em questão sofreu veto, ainda sendo pendente sua votação.

GDPR - General Data Protection Regulation:

A *General Data Protection Regulation* é a legislação da União Europeia que aborda o tratamento de dados e sua livre circulação. A LGPD, que se inspirou na GDPR, tem como finalidade proteger os dados pessoais dos **Usuários da internet** , trazer regulações relacionadas ao seu tratamento, armazenamento, direitos, garantias e uso.

Assim como a LGPD, a GDPR também regula decisões automatizadas. Em seu artigo 22, o legislador estabelece que o titular dos dados tem direito a não ser sujeitado a decisões tomadas exclusivamente com base em tratamento automatizado. São tidas como exceções as decisões baseadas em consentimento explícito do titular, autorizadas por legislação específica local ou decisões necessárias à execução ou celebração de contrato entre o titular dos dados e o responsável por seu tratamento

CDC – Código de Defesa do Consumidor:

No caso das relações entre o titular dos dados e entidades privadas que fazem uso de decisões automatizadas, como, por exemplo, para cessão de crédito, o quesito transparência é fundamental e transversal ao início de uma construção legislativa sobre a regulação de algoritmos no Brasil. No entanto, a opacidade desses sistemas é a regra (WAGNER, 2016), em desacordo com uma série de dispositivos do Código de Defesa do Consumidor, entre eles o Artigo6º, inc. III, e Artigo 31 (informações claras, adequadas e precisas, bem como os riscos); Artigo 43 (acesso aos dados pessoais existentes sobre si em bancos de dados e

cadastros, bem como as respectivas fontes); e Artigo 43, §1º, inc. II (nulidade das cláusulas que ofendam direitos inerentes à natureza do contrato, ameaçando seu equilíbrio - como o direito de revisão). Em se tratando das correlações entre a disciplina consumerista e a práxis cultural do desenvolvimento de algoritmos, um longo caminho deverá ser trilhado para o estabelecimento de um arcabouço legal protetivo ao titular dos dados.

Acquisition of Surveillance Technology:

A avaliação a *posteriori* das decisões tomadas por algoritmos parece ser a tônica geral das regulações de inteligência artificial. Isso preocupa, pois, das variadas aplicações de processos automatizados por algoritmos, sobretudo com base em identificação biométrica, a vigilância governamental passa a carregar escalas inéditas de potenciais violações aos direitos humanos (*ACCESS NOW*, 2018). Reconhecimento facial para o monitoramento de etnias (*JOSEPH*, *LIPP*, 2018) e dissidentes políticos (*JOSEPH*, 2019), predição de intenções terroristas (*UCLA*, 2017), *score* social (*KOBIE*, 2019), e até predição criminal (*ANGWIN et al*, 2016) são algumas das inúmeras aplicações para finalidades de vigilância que vêm tensionando o uso de tecnologias e seus aspectos sociopolíticos.

Sobre a questão, é interessante apontar para a regulação do uso de tecnologias de vigilância da cidade de São Francisco. Entendendo serem os efeitos colaterais à garantia de direitos - como a **Privacidade** e a não discriminação - o ponto de partida para o debate público, a proposta prevê que entidades policiais, sempre que pretenderem implementar nova tecnologia de vigilância - sobretudo inteligências artificiais -, elaborem uma política prévia que comprove que os benefícios à segurança pública irão superar os danos aos direitos humanos. Este relatório deve ser, então, avaliado por um Conselho local, com a participação da sociedade civil, antes da efetiva aplicação.

Princípios:

Primeiramente, é importante observar que grande parte dos princípios são autoexplicativos e estão expressos nos incisos do Artigo 6º. Os incisos V, VI, IX e X, do referido dispositivo se interligam diretamente ao direito de revisão

automatizada, e para melhor compreensão vamos descrevê-los de forma simplificada a seguir.

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*." Esse inciso é bastante autoexplicativo quando demonstra que os dados sejam exatos, claros e passíveis de atualização para que se possa cumprir a finalidade indicada e consentida.

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." Garante que os titulares possam buscar informações sobre seus dados, devendo ser claras e facilmente acessíveis. Com isso, você poderá solicitar seus dados, corrigi-los e até mesmo pedir sua exclusão de forma rápida, fácil e descomplicada.

IX – "**não discriminação**: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos." Os dados coletados não podem categorizar cor, raça, religião, opinião política que tenham como tendência a discriminação.

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." A empresa ou órgão deverá prestar contas, quando solicitados, quanto ao cumprimento da LGPD e caso haja descumprimento de qualquer ponto da lei caberá a responsabilização.

PROBLEMÁTICA

A ***Lei Geral de Proteção de Dados Pessoais***, em seu artigo 20, prevê o direito de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, em que o controlador deve disponibilizar as informações necessárias sobre os critérios e procedimentos usados na decisão automatizada, sendo observados os segredos industriais.

Com isso, o artigo deferido traz uma série de questionamentos e preocupações acerca da utilização dos algoritmos para a produção de

julgamentos sobre as pessoas, nos quais são dependentes do acesso aos dados pessoais da população. Logo, os direitos previstos no artigo 20 da LGPD são direcionados à problemática de estarem dependentes do alinhamento com o segredo industrial. Entretanto, na GDPR (*General Data Protection Regulation*), os segredos industriais não são explicitados, são tratados de forma objetiva e concisa.

Não obstante, se, por algum motivo o controlador não ceder as informações referentes ao §1º do artigo mencionado, mais uma vez, zelado o segredo industrial, a Autoridade Nacional poderá realizar auditorias para tratamento dos dados pessoais. Por isso, é de significante importância a atuação da ANPD na prevenção de problemas, pois o dano individual refletido nos cidadãos, ao terem seus dados vazados, comparados com qualquer **Sanção** sofrida pelo órgão responsável por tal ato, é tida como mais grave e irreversível.

Com a aprovação da **Lei n. 13.853/19**, a LGPD sofreu alterações importantes. Dentre essas alterações temos o veto presidencial ao §3º, do Artigo 20, da LGPD, que atingiu regras para a revisão de decisões automatizadas, que podem ir desde a retirada de um conteúdo de uma rede social à concessão ou não de crédito a uma pessoa. O texto aprovado pelo congresso conferia ao cidadão o direito de solicitar essa revisão, e observava que este procedimento só poderia ser realizado por pessoa natural. Com o veto, essa obrigação desaparece.

Esta era a grande polêmica no período de tramitação da **MP 869/2018**, posteriormente convertida em lei, no Congresso Nacional. Pois argumentava-se que algoritmos revisando algoritmos trariam risco aos cidadãos, enquanto por outra ótica, ***Startups*** e empresas de TI alegavam prejuízo direto ao seu modelo de negócio, em especial em relação a inteligência artificial e *big data*.

A justificativa do presidente para o veto é de que a revisão humana "*contraria o interesse público*", uma vez que "*inviabilizará os modelos atuais de planos de negócios de muitas empresas, notadamente das startups, bem como impacta na análise de risco de crédito e de novos modelos de negócios de instituições financeiras, gerando efeito negativo na oferta de crédito aos consumidores*".

No entanto, o veto ainda poderá ser derrubado. No cenário atual a tentativa de votação acerca do veto restou infrutífera, vez que não houve quórum suficiente para submeter o assunto em pauta a votação.

André Ramiro
Diretor do IP.rec - Instituto de Pesquisa em Direito e Tecnologia do Recife. Atualmente, é o Latin America Google Policy Fellow na ONG Derechos Digitales (Chile). Mestrando em Ciências da Computação no CIn/UFPE e formado em Direito pela UFPE. Formado pela Escola de Governança da Internet do Comitê Gestor da Internet (CGI.br).

Barbara Santini Pinheiro
Advogada. Graduada em Direito pela Universidade Católica de Pernambuco (UNICAP). Pesquisadora do PlacaMae.Org_. Pós-graduanda em Direito Civil e Processo Civil pela ESA. Membro colaboradora da Comissão de Direito e Tecnologia da Informação da OAB-PE.

Genifer de Andrade Silva Lima
Advogada. Pós-graduada em Direito Administrativo pela Universidade anhanguera uniderp Graduada em Direito pela Faculdade de Joaquim Nabuco Pesquisadora do Placamãe.org_ Membro da Comissão de Direito e Tecnologia da Informação da OAB/PE.

João Paulo Borba Maranhão
Advogado, graduado pela Universidade Católica de Pernambuco e pós-graduando em Compliance Digital pela Universidade Presbiteriana Mackenzie. Interessado em direito digital, direito à privacidade na era da informação e inovações tecnológicas aplicadas ao meio jurídico, entre outros vários temas ligados a direito e tecnologia.

Tatiana Caroline Lucena de Medeiros Gonçalves
Graduanda em Direito pela Universidade Católica de Pernambuco; Membro da Comissão de Direito e da Tecnologia da Informação da OAB/PE.

Thaís Helena Carneiro Barros Aguiar
Estudante de Direito na Universidade Federal de Pernambuco, membro do IP.rec - Instituto de Pesquisa em Direito e Tecnologia de Recife e membro colaboradora da Comissão de Direito da Tecnologia e da Informação.

Referências

- WORLD ECONOMIC FORUM. **The Fourth Industrial Revolution: what it means, how to respond.** Disponível em: <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/>. Acesso em: agosto de 2019.
- INTERNET WORLD STATS. **Internet Usage Statistics**. Disponível em: <https://www.internetworldstats.com/stats.htm>. Acesso em: agosto de 2019. Dados recolhidos da Divisão Populacional das Nações Unidas e da União Internacional de Telecomunicações.
- COOKE, Roger L. (2005). **The History of Mathematics: A Brief Course**. John Wiley & Sons.
- MOSCHOVAKIS Y.N. **What Is an Algorithm?** In: Engquist B., Schmid W. (eds) Mathematics unlimited: 2001 and Beyond. Springer, Berlin, Heidelberg, p. 919-936.
- CASTELLS, Manuel; ESPANHA, Rita. **A era da informação: economia, sociedade e cultura.** Paz e terra, 1999.
- CORMEN, Thomas H. et al. **Introduction to algorithms**. MIT press, 2009, p. 14.

- LOHR, Steve**. The age of big data.** New York Times, v. 11, n. 2012, 2012.
- PROVOST, Foster; FAWCETT, Tom. **Data science and its relationship to big data and data-driven decision making.** Big data, v. 1, n. 1, p. 51-59, 2013.
- KAPLAN, Andreas; HAENLEIN, Michael. **Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence.** Business Horizons, v. 62, n. 1, p. 15-25, 2019.
- AHA, David W.; KIBLER, Dennis; ALBERT, Marc K. **Instance-based learning algorithms**. Machine learning, v. 6, n. 1, p. 37-66, 1991.
- WAGNER, Ben. **Algorithmic regulation and the global default: shifiting norms in Internet technology**. Nordic Journal of Applied Ethics, 2016, págs 5-13.
- Human Rights in the Age of Artificial Intelligence. Access Now, 2018. Disponível em https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf. Acesso em 27 de agosto de 2019.
- JOSEPH, George. LIPP, Kenneth. **IBM used NYPD surveillance footage to develop technology that lets police search by skini color.** The Intercept, 2018. Disponível em https://theintercept.com/2018/09/06/nypd-surveillance-camera-skin-tone-search/. Acesso em 27 de agosto de 2019.
- JOSEPH, George**. Inside video surveillance program IBM built for philippine strongman Rodrigo Duterte.** The Intercept, 2018. Disponível em https://theintercept.com/2019/03/20/rodrigo-duterte-ibm-surveillance/. Acesso em 27 de agosto de 2019.
- **Bad Trip: debunking the TSA's 'behavior detection' program.** UCLA - American Civil Liberties Union, 2017. Disponível em https://www.aclu.org/report/bad-trip-debunking-tsas-behavior-detection-program?redirect=bad-trip. Acesso em 27 de agosto de 2019.
- KOBIE, Nicole. **The complicated truth about China's social credit system.** WIRED, 2019. Disponível em https://www.wired.co.uk/article/china-social-credit-system-explained. Acesso em 27 de agosto de 2019.
- Angwin,J., Larson,J., Mattu,S. & Kirchner,L., Machine Bias. (2016). **There is software that is used across the county to predict future criminals. And it is biased against blacks.** Disponível em: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. Acesso em: 27 out. 2019
- BRASIL. Presidência da República. Lei nº 13.853, de 8 de julho de 2019. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/Lei/L13853.htm Acesso em: 25 out. 2019
- BRASIL. Presidência da República. Medida Provisória nº 869, de 27 de dezembro de 2018. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Mpv/mpv869.htm. Acesso em: 29 out. 2019

Capítulo 8

Dos agentes de tratamento de dados pessoais

Bruna Mattos
Genifer Andrade
Hélio Batista
Leonardo Lumack

A ***Lei Geral de Proteção de Dados Pessoais***[10] elenca e define, em seu artigo 5º, incisos VI[11], VII[12], VIII[13] e IX[14], as figuras dos agentes de **Tratamento** de **Dados pessoais**, quais sejam, o controlador e o operador. Não obstante, a lei também traz a figura do encarregado, cuja definição e limites de atuação veremos adiante.

Conforme se verifica da leitura dos referidos dispositivos, considera-se controlador aquele sujeito que é pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Já o operador é pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Por fim, o encarregado, que é a pessoa indicada pelo controlador e pelo operador (nos casos indicados pela **Autoridade Nacional de Proteção de Dados – ANPD** , conforme disposto no artigo 41, §3º[15], da LGPD) para atuar como canal de comunicação entre o controlador, os **titulares** dos dados e a Autoridade Nacional de Proteção de Dados - ANPD.

---

[10] BRASIL. **Lei n. 13.709**, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados (LGPD)**. (Redação dada pela Lei n.13.853 de 2019 que altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências). Diário Oficial da União, Brasília, 15 ago. 2018.

[11] VI - **Controlador**: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

[12] VII - **Operador**: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

[13] VIII - **Encarregado**: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

[14] IX - **Agentes de tratamento**: o controlador e o operador;

[15] **Artigo 41.** O controlador deverá indicar encarregado pelo tratamento de dados pessoais. **§ 3º** A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

Fonte: www.a2c.com.br/novidade/lgpd-no-marketing-digital/

Com base nestas definições legais, conclui-se, de pronto, que o controlador é o principal tomador das decisões que envolvem os dados pessoais coletados. Ele determina a razão da coleta dos dados; controla como eles serão coletados e posteriormente usados; seleciona quais dados serão coletados, bem como quem terá seus dados coletados; define quanto tempo esses dados permanecerão armazenados; e estabelece quem terá acesso a esses dados. Ademais, é ele o maior responsável por proteger os dados dos titulares e como consequência direta, a maior parte das responsabilidades previstas na LGPD também incidirão sobre ele.

No que tange ao operador de dados, diz a lei que se trata da pessoa natural ou jurídica responsável por processar dados pessoais em nome do controlador. É ele quem realiza o tratamento de dados nos termos do que determinado pelo controlador. O operador não controla os dados e nem pode alterar a finalidade ou o seu uso, limitando-se ao processamento daqueles em conformidade com as determinações e o propósito designado pelo controlador.

Não obstante as limitações acima, o operador terá liberdade para decidir qual o sistema, o método e as ferramentas que serão aplicados na coleta dos dados, além de definir como eles serão armazenados. O operador deverá ainda garantir a segurança destes, dos meios utilizados para transferi-los de uma organização para outra e das ferramentas aplicadas para recuperá-los.

Por último, a lei prevê a figura do encarregado pelo tratamento de dados, conhecido na ***GDPR - General Data Protection Regulation*** europeia como DPO

(*Data Protection Officer*). O encarregado, pessoa física ou jurídica, tem como missão receber as reclamações e comunicações dos titulares dos dados, bem como prestar os devidos esclarecimentos e garantir que sejam tomadas as medidas necessárias ao cumprimento das regras e das boas práticas de proteção de dados. Deverá, ainda, receber comunicações da autoridade nacional de proteção de dados (ANPD) e adotar as providências eventualmente exigidas, bem como orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.

Não obstante a ausência de previsão legal, deverá o encarregado executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares, desde que não o coloque em posição de conflito de interesse com o desempenho de suas atividades legais. No entanto, a LGPD não definiu a abrangência de suas funções ou a formação necessária para exercer o cargo de encarregado de dados.

Recomenda-se, contudo, dos profissionais que desejam exercer essa função, conhecimentos técnicos e jurídicos na área, além de competências interpessoais que vão oscilar de acordo com a necessidade da empresa. Afinal de contas, a constante evolução tecnológica e o amplo acesso à informação trazem constantes desafios quando falamos de proteção de dados, o que resulta numa série de ações para garantir a segurança da informação. E assim, uma vez responsável pelos processos de manipulação de dados pessoais dentro da empresa, o encarregado acabará contribuindo também com outras áreas.

Dentre as várias atribuições **e responsabilidades dos agentes de tratamento** previstas na LGPD, elencamos as seguintes:

1 - Observância dos princípios gerais e da garantia dos direitos do titular (Artigo 7º, §6º);

2 - Obter consentimento, quando necessário (Artigo 7º, §5º; Artigo 8º, §6º);

3 - Informar e prestar contas;

4 - Garantir a portabilidade (Artigo 9º; Artigo 18; Artigo 20);

5 - Garantir a transparência no tratamento de dados baseado em legítimo interesse (Artigo 10, §2º);

6 - Manter registro e manutenção das operações de tratamento de dados pessoais, especialmente quando baseado no legítimo interesse (Artigo 37);

7- Elaborar relatório de impacto à proteção de dados pessoais, inclusive de **Dados sensíveis**, referente a suas operações de tratamento de dados, com observância dos segredos comercial e industrial (Artigo 10; §3º; Artigo 38);

8 - Indicar o encarregado pelo tratamento de dados (Artigo 41);

9 - Reparar danos patrimoniais, morais, individuais ou coletivos causados por violação à legislação de proteção de dados pessoais (Artigo 42 e 44, Parágrafo único);

10 – Adotar medidas de segurança, técnicas e administrativas (artigo 46);

11 - Garantir a segurança da informação em relação aos dados pessoais, mesmo após o seu término (Artigo 47);

12 - Comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (Artigo 48);

13 - Salvaguardar os direitos dos titulares mediante a adoção de providências, como, por exemplo, a divulgação do fato em meios de comunicação e medidas para reverter ou mitigar os efeitos do incidente (Artigo 48, §2º);

14 – Formular regras de boas práticas e de governança (Artigo 50).

Fonte: http://fundacaotelefonica.org.br/educacao-do-seculo-xxi/lei-geral-de-protecao-de-dados-pessoais-por-que-sua-escola-precisa-se-preocupar/

Dentre todas essas atribuições e responsabilidades acima elencadas, entendemos merecer atenção especial a aplicação do princípio da boa-fé como guia para a atuação dos agentes de tratamento de dados. Todos os princípios dispostos no Artigo 6º[16] da LGPD são extremamente relevantes, mas vale registrar que, no tocante ao controlador e o operador, o princípio da boa-fé previsto em seu *caput* merece singular destaque em face das atribuições legais dos referidos agentes de tratamento de dados previstas no Artigo 5º, incisos VI e VII, respectivamente.

Fonte: https://www.portaldaprivacidade.com.br/post/infogr%C3%A1fico-04-os-10-princ%C3%ADpios-para-o-tratamento-de-dados-pessoais

[16] **Artigo 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.

Por ser um dos princípios fundamentais do direito privado, a sua função é estabelecer um padrão ético de conduta dos referidos agentes de tratamento para com os titulares de dados, sobretudo com relação à predominância do respeito aos direitos conexos, dentre eles os deveres de cuidado em relação ao titular, de respeito, de informação sobre o conteúdo do negócio, de probidade, de colaboração e de agir conforme a confiança depositada, com honestidade, de forma razoável e com equidade. Qualquer ofensa a qualquer um dos referidos deveres implica, necessariamente, em ofensa ao princípio da boa-fé.

Considerando a confiança depositada pelo titular aos agentes de tratamento mediante o cumprimento do previsto no Artigo 7º, inciso I[17], esse autoriza os respectivos agentes a procederem com o tratamento dos seus dados, respeitadas as limitações da lei.

Podemos destacar como exemplos de importância da predominância do princípio da boa-fé por parte dos agentes de tratamento os seguintes dispositivos:

a) Artigo 7º, §5º: Caso o controlador tenha que comunicar ou compartilhar dados pessoais já em tratamento, necessário se fará um consentimento para tal fim, ressalvado as exceções da lei;

b) Artigo 8º, §5º: O consentimento para tratamento dos dados poderá ser revogado pelo titular a qualquer tempo, devendo o controlador paralisar todo o tratamento previsto no Artigo 5º, X;

c) Artigo 9º, §2º: Uma vez já formalizado o consentimento inicial, caso a finalidade inicial do tratamento dos dados seja modificada, caberá ao controlador pedir autorização ao titular de dados;

[17] **Artigo 7º** O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular;

d) Artigo 18º, VI: O titular de dados tem direito de obter do controlador a efetiva eliminação dos seus dados pessoais.

Os exemplos acima evidenciam claramente a necessidade de o titular de dados confiar no controlador para situações extremamente importantes.

No entanto, reportando-nos aos dispositivos supracitados, verifica-se que tais expedientes, cabíveis exclusivamente ao controlador e, por via de consequência, a eventual operador, evidenciam uma necessidade desses agentes de tratamento de satisfazerem por completo a confiança depositada pelo titular dos dados na ocorrência de qualquer das referidas previsões.

Ademais, vale registrar, quanto ao dado pessoal tratado em banco de dados eletrônico, no tocante a possibilidade da eliminação prevista no Artigo 18º, inciso VI[18], por exemplo, a confiança plena do titular de dados se apresenta com destaque com relação ao controlador.

Afinal de contas, ao requerer a eliminação de todos os seus dados pessoais junto ao acervo eletrônico do controlador, o titular, a princípio, confiará na simples afirmação desse último, não havendo possibilidade técnica, a nosso ver, de que o agente de tratamento prove cabalmente que o dado virtual foi efetivamente eliminado, prevalecendo, nesse caso, a plena confiança do titular de dados na afirmação do controlador, sendo mais uma razão da importância do princípio da boa-fé nessa relação entre titular e agentes de tratamento.

O operador, por ser agente que realiza tratamento de dados em nome do controlador, se encontra num grau de importância igualmente relevante nesse processo, estando presente o princípio da boa-fé de forma muito enfática no contexto da relação entre titular de dados, controlador e operador.

Destaque-se, por fim, que o tratamento de dados não surgiu em nosso ordenamento jurídico com a LGPD. A Lei nº12.527/2011[19] já previa algumas

[18] **Artigo 18**. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no Artigo 16 desta Lei;

[19] BRASIL. **Lei n.12.527**, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do artigo 5º, no inciso II do & 3º do art. 37 e no & 2º do art.216 da Constituição Federal; altera a Lei n.8.112, de 11 de dezembro de 1990; revoga a lei n.11.111, de 5 de maio de 2005, e dispositivos da Lei n. 8.159,de 8 de janeiro de 1991; e dá outras providências. Diário Oficial da União, Brasília, 19 nov. 2011

disposições referentes ao tratamento de dados por parte das pessoas jurídicas previstas no seu Artigo 1º, §único, incisos I e II[20], bem como no seu Artigo 2º[21], restando como necessário esse tratamento no exercício de suas atividades com o objetivo de garantir proteção ao titular do dado, conforme previsão do Artigo 31[22], o qual especifica que o tratamento da informação pessoal deve ser feita de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.

Como forma de corroborar a importância de garantia a essa proteção, o inciso II[23] do referido dispositivo nos traz a necessidade de consentimento expresso do titular da informação para que ela seja divulgada ou acessada por terceiro. Dessa forma, no tocante ao âmbito público, já existia na nossa legislação normas visando a garantia da proteção dos dados pessoais de qualquer interessado.

Bruna Mattos

Advogada na área Empresarial com ênfase em societário e proteção de dados pessoais no escritório Caribé Advogados. Bacharela em Direito pela Universidade Federal de Pernambuco - UFPE. Formada no programa de gestão, liderança e empreendedorismo (EMPRETEC) pelo SEBRAE/PE. Sócia Titular e Fundadora da Qualimetra - Medicina Ocupacional. Pós-graduada em Direito Civil e Empresarial pela Universidade Federal de Pernambuco. Formada no curso de Privacidade e Proteção de Dados pelo INSPER/SP e pelo ITS/RJ.

Genifer de Andrade Silva Lima

Advogada. Pós-graduada em Direito Administrativo pela Universidade anhanguera uniderp; Graduada em Direito pela Faculdade de Joaquim Nabuco; Pesquisadora do Placamãe.org_; Membro da Comissão de Direito e Tecnologia da Informação da OAB PE.

[20] **Artigo 1º** Esta Lei dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do Artigo 5º , no inciso II do § 3º do Artigo 37 e no § 2º do Artigo 216 da Constituição Federal. Parágrafo único. Subordinam-se ao regime desta Lei: I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público; II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

[21] **Artigo 2º** Aplicam-se as disposições desta Lei, no que couber, às entidades privadas sem fins lucrativos que recebam, para realização de ações de interesse público, recursos públicos diretamente do orçamento ou mediante subvenções sociais, contrato de gestão, termo de parceria, convênios, acordo, ajustes ou outros instrumentos congêneres.

[22] **Artigo 31**. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.

[23] **II** - Poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.

Hélio André Medeiros Batista

Advogado inscrito no Brasil e em Portugal, pós-graduado em Direito Civil, Empresarial e Ambiental. Especialista em Direito Empresarial, Societário e Compliance Digital. Conselheiro do Instituto Brasileiro de Política e Direito da Informática - IBDI e membro da Comissão de Direito e da Tecnologia da Informação da OAB/PE.

Leonardo Lumack do Monte Barretto

Pós-graduado pela Escola Superior da Magistratura de Pernambuco - ESMAPE; Especialista em Direito Civil e Empresarial; Especialista em Direito Digital e Compliance; Conselheiro do Instituto Brasileiro de Direito da Informática - IBDI; membro da Comissão de Direito e Tecnologia da Informação da OAB-PE.

Capítulo 9

Autoridade Nacional de Proteção de Dados (ANPD)

Aline Menezes
André Campello
Antônio Araújo Junior
Camila Vilela
Daniel Guimarães

Com uma pequena defasagem em relação à promulgação da ***Lei Geral de Proteção de Dados Pessoais* (LGPD),** foi editada a lei que cria autoridade nacional de proteção de dados, a Lei Federal n.º 13.853/2019, que surgiu da conversão da Medida Provisória n.º 869/2018. Dessa forma, conforme o artigo 55 da referida LGPD, a Autoridade Nacional de Proteção de Dados Pessoais (ANPD) é um órgão integrante da administração pública que faz parte da estrutura da Presidência da República, possuidora de autonomia técnica.

É importante lembrar que a regulamentação da proteção de dados gera um alto impacto em todos os âmbitos da sociedade. Tem força impactante tal quanto outras legislações de relevante importância como o **Código de Defesa do Consumidor**, a Lei de Acesso à Informação (LAI) e a Lei de Crimes Ambientais, pois na sociedade da informação cada vez mais os dados são de alguma maneira tratados e utilizados.

Mais especificamente quanto a Autoridade Nacional de Proteção de Dados (ANPD), inspirada na legislação de vanguarda advinda da Europa, a LGPD instituiu o órgão como elemento central e fundamental na interpretação e fiscalização da lei. Nesse sentido, desempenhará a tarefa de orientar, por meio de seu corpo técnico especializado, todos os agentes da sociedade sobre quais os limites e vicissitudes do texto legal, especificando do ponto de vista prático a concretização dos conceitos abstratos e indeterminados que permeiam o diploma. Além disso, a ANPD irá cooperar com as autoridades de controle de proteção de dados de

outros Estados, nomeadamente na defesa e no exercício dos direitos de pessoas residentes no estrangeiro.

No passo, é válido ressaltar que a análise da atuação da ANPD deve passar pela **evolução histórica** e **normativa**, vislumbrando o surgimento e a maturidade do **Tratamento** de dados, o que necessariamente passa pela análise dos seguintes diplomas legais:

- *CDC;*
- *Lei de interceptação Telefônica e Telemática;*
- *Lei Geral de Telecomunicações;*
- *Lei do Habeas data;*
- *Lei do Crime de inserção de dados falsos em sistemas de informações da administração pública;*
- *Lei n.º 12.414/2011, que disciplinou o cadastro positivo;*
- ***Lei de Acesso à Informação** ;*
- *Decreto 7.962/2013, que regulamentou o comércio eletrônico;*
- *Marco Civil da Internet e seu decreto regulamentador e, por fim,*
- *Medida Provisória n.º 869/2018, que criou a ANPD.*

Todos esses diplomas servirão de base teleológica para interpretação, aplicação e valoração da atuação do órgão, principalmente neste momento inicial, em que as eventuais lacunas serão supridas.

Este presente trabalho focou **exclusivamente** na Medida Provisória que originou a Lei que cria a Autoridade Nacional de Proteção de Dados, fazendo um breve transcurso nos capítulos II - Tratamento de **Dados pessoais**; IV - Tratamento de Dados Pessoais pelo Poder Público; VI - Dos Agentes de Tratamento de Dados Pessoais; VIII - Da Fiscalização e IX - Da Autoridade Nacional de Proteção de Dados e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, e, por fim, pela Lei Federal n.º 13.853/2018, que criou a ANPD.

Impende destacar, ainda, que a análise deve ser feita sobre o prisma dos fundamentos e princípios elencados na **Constituição Federal** e no **Marco Civil da Internet**, bem como nos princípios que incidem sob a atuação dos órgãos administrativos.

A MEDIDA PROVISÓRIA N.º 869/2018

As medidas provisórias, que possuem força de lei, são instrumentos legais lançados mão pelo Presidente da República em casos de relevância e urgência, com submissão ao Congresso Nacional (Artigo62, da CR/88). Neste sentido, o Presidente da República editou a Medida Provisória n.º 869/2018, a fim de implantar a nova sistemática a ser seguida pelo Poder Público para proteção dos dados.

Por meio da mensagem n.º 789/2018, o Poder Executivo submeteu à análise do Congresso Nacional a MP, na qual restou verificado o atendimento aos pressupostos de **urgência** e **relevância** dos assuntos tratados; a constitucionalidade, juridicidade e técnica legislativa da matéria, bem como foram analisados os resumos das audiências públicas e o mérito da matéria.

Diversos questionamentos e sugestões foram apresentados nas audiências públicas que sucederam a aprovação da conversão da MP em Lei. Destaque-se, por exemplo, as seguintes questões em torno de sua criação:

i. **A ANPD é vinculada à administração pública direta e à Presidência da República**. Criação de um regime híbrido. A questão envolve a urgência na criação do órgão em confronto com a impossibilidade do aumento da despesa e a necessidade de independência da ANPD. Havia forte receio de que a imposição da ANPD nascer já como autarquia gerasse maior impasse legislativo, com o congresso impondo novos vetos, o que atrasaria sua criação e acarretaria um vácuo jurídico de autoridade para regular e fiscalizar o tratamento de dados no Brasil. (A manutenção da ANPD na estrutura da Presidência da República possui como ganho operacional a sua rápida implantação, tendo em vista a não possibilidade de recusa de cessão de recursos humanos para formação do corpo técnico da entidade.);

ii. **A composição do órgão**. Sabatina pelo Senado Federal empresta maior legitimidade ao mandato dos diretores da ANPD;

iii. **Alteração do dispositivo que previa o afastamento de conselheiro pelo Presidente da República**. Eventual afastamento deverá ser decidido por comissão especial criada para apurar processo administrativo disciplinar

iv. A transformação da ANPD em autarquia no prazo de dois anos a partir da aprovação de sua estrutura regimental, bem como a tempo de ser incluída nas leis orçamentárias.

v. Competência para decidir. Competência para elaboração do regimento interno. Regimento interno aprovado pelo presidente.

vi. Atribuições da ANPD. A Medida Provisória **exclui** algumas atribuições que constavam na lei aprovada pelo Congresso Nacional, dentre as quais listamos as seguintes:

(a) zelar pela observância dos segredos comercial e industrial em ponderação com a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do Artigo 2º da LGPD;
(b) elaborar diretrizes para Política Nacional de Proteção de Dados Pessoais e da Privacidade;
(c) atender petições de titular contra responsável;
(d) dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, observado o respeito aos segredos comercial e industrial;
(f) 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, podendo emitir parecer técnico complementar;
(g) arrecadar e aplicar suas receitas e publicar no relatório de gestão o detalhamento de suas receitas e despesas; e
(h) realizar ou determinar a realização de auditorias, no âmbito da atividade de fiscalização, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluindo o poder público.

Ficou decidido pela imprescindibilidade da restauração das atribuições da ANPD, tais como previstas na Lei originalmente aprovada pelo Congresso Nacional, para o bom funcionamento da agência e a efetiva proteção dos dados pessoais. Ademais, decidiu-se pela adição contidas na MP, mais especificamente quanto a:

(a) deliberar de maneira definitiva na esfera administrativa;
(b) requisitar informações a qualquer momento;
(c) comunicar às autoridades infrações penais e o descumprimento desta Lei pela Administração;

(d) a promoção de estudos; e
(e) articular-se com demais reguladoras públicas.

Por fim, entenderam pela pertinência da possibilidade da celebração de termo de ajustamento de conduta (TAC) e de dar publicidade aos relatórios da instituição.

A ANPD COMO AGENTE ADMINISTRATIVO

A criação da ANPD já estava prevista na Lei Geral de Proteção de Dados, porém, como antedito, no intuito de impedir quaisquer questionamentos acerca de sua constitucionalidade, a ANPD foi criada por meio da MP 869/2018. Esperava-se, a princípio, um órgão mais independente, com autonomia administrativa e personalidade jurídica própria. No entanto, a ANPD fora criada como órgão da administração pública federal, integrante da Presidência da República, e sob a premissa de contenção de gastos, o que denota um certo descaso do Governo com um tema de extrema relevância.

Em que pese, a princípio, a ausência de autonomia administrativa, a MP 869/2018, ao menos, assegurou a autonomia técnica do órgão, visando uma atuação em melhores condições, privilegiando a técnica exigida em detrimento dos interesses políticos e lobísticos que permeiam a atuação das entidades que detêm o poder de regulamentar e fiscalizar. Ainda assim, muito dos dispositivos aplicáveis à Autoridade Nacional serão objeto de regulação pelo regimento interno da entidade.

Nesse aspecto, é interessante destacar que, a exemplo do CADE e do PROCON no âmbito Federal, as arrecadações decorrentes de multas serão destinadas ao FDD (Fundo de Defesa dos Direitos Difusos), o que em certa medida supostamente desafetaria as decisões e sanções administrativas de eventual sanha arrecadatória.

Diferentemente de outros órgãos fiscalizadores, com atuação basicamente performada no poder de polícia, a ANPD exercerá também o Poder Regulamentar, o que lhe possibilita a edição de normas que envolvam o cumprimento prático dos dispositivos e princípios elencados na LGPD.

Com o objetivo de assegurar a observância das diretrizes impostas aos Controladores e Operadores - nos termos da referida lei, obrigados a reparar eventuais danos causados ao titular -, há as aplicações das sanções administrativas pela Autoridade Nacional de Proteção de Dados (ANPD).

Nesse sentido, investida do poder de polícia, a autoridade nacional deve atuar para assegurar o perfeito equilíbrio entre os direitos individuais e o interesse público, com destaque para (Artigo55-J):

> I - Zelar pela proteção dos dados pessoais, nos termos da legislação;
> 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; e
> VI - Promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança.

Acontece que a atividade administrativa sancionadora é reflexo do poder punitivo estatal e, portanto, impõe-se a observância das garantias penais de estatura constitucional. Assim, na interpretação das sanções administrativas aplicáveis pela ANPD, previstas nos artigos 52 a 54, da LGPD, princípios como a proibição de interpretação extensiva e de analogia *in malam partem* devem ser tomados em consideração.

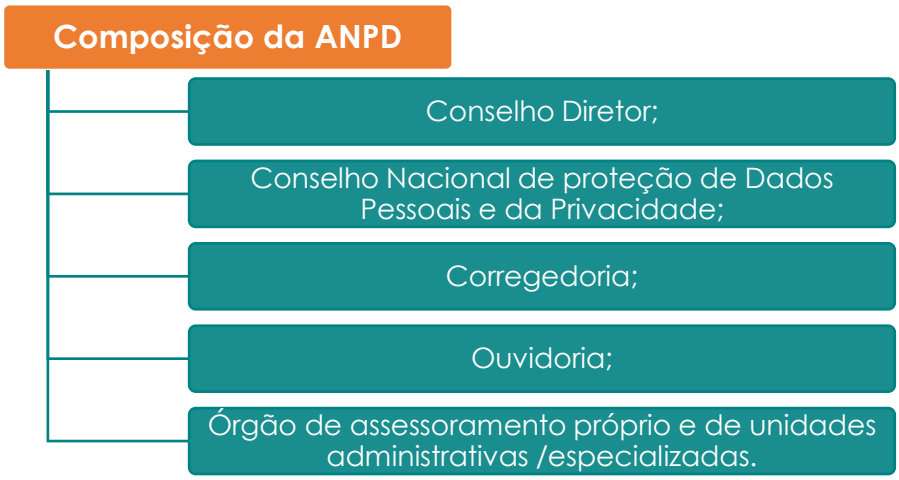
É consenso que a LGPD terá impacto importante nas operações de tratamento de dados pessoais por empresas que atuam no Brasil e considerando as preocupações que têm sido levantadas com a concentração de dados pessoais para uso comercial, é de se esperar que haja não só interação mas coordenação entre ANPD e os órgãos de defesa do consumidor, como também com o CADE (Conselho Administrativo de Defesa Econômica), que tem por função aplicar a Lei de Defesa da Concorrência (lei 12.529/11). Foi visando evitar que setores específicos da atividade econômica fossem profundamente atingidos que o §2º do Artigo 55-J, dispõe sobre a necessidade de coordenação da atividade.

O poder regulamentar, fundado na premissa da intervenção mínima, possibilita à administração gerar normas que possibilitam o cumprimento de uma

lei ou norma. Visa, portanto, alcançar os detalhes práticos que envolve o tratamento de dados e não poderiam ser observados pelo legislador, dada a particularidade envolvida na ciência e técnicas. Mesmo assim, restou delineado na Medida Provisória o arcabouço dessa atuação, segundo a qual já resta prevista a formulação de Boas Práticas e Governança, *Compliance* e gestão de risco e Padrões técnicos de segurança e sigilo – tal como o ***Privacy by design*** -, sempre privilegiando o titular do dado.

Neste sentido, não restam dúvidas quanto a necessidade de mudança na cultura do tratamento de dados no Brasil e a medida da mudança decorrerá da atuação da autoridade. Isso porque, sobretudo, vale ressaltar que a LGPD é considerada uma carta principiológica, assim, regras e balizas gerais serão regulamentadas pela futura ANPD.

A ATUAÇÃO DA ANPD



O Conselho Diretor da ANPD, que é o órgão máximo de direção, é composto por cinco diretores nomeados pelo então Presidente da República, que são escolhidos dentre brasileiros que possuem reputação ilibada, com nível superior de educação e elevado no conceito no campo de atuação, para que sejam almejados para o cumprimento de um mandato de quatro anos.

O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade é composto por 23 (vinte e três) representantes sendo 5 (cinco) do Poder Executivo

federal; 1 (um) do Senado Federal; 1 (um) da Câmara dos Deputados; 1 (um) do Conselho Nacional de Justiça; 1 (um) do Conselho Nacional do Ministério Público; 1 (um) do Comitê Gestor da Internet no Brasil; 3 (três) de entidades da sociedade civil com atuação relacionada a proteção de dados pessoais; 3 (três) de instituições científicas, tecnológicas e de inovação; 3 (três) de confederações sindicais representativas das categorias econômicas do setor produtivo; 2 (dois) de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais e 2 (dois) de entidades representativas do setor laboral. (Artigo58-A, da Lei nº13.709/2018).)

A ANPD é um mecanismo de atuação da LGDP com a função principal de zelar pela proteção de dados pessoais através das competências normativa, deliberativa, fiscalizadora e sancionatória. E tem como principal competência "zelar pela proteção dos dados pessoais" (Artigo 55-J, inc. I). Para isso, suas competências mais relevantes são: "editar normas e procedimentos sobre a proteção de dados pessoais" (inc. II); deliberar sobre a interpretação da LGPD, suas competências e os casos omissos (inc. III); requisitar informações aos controladores e operadores de dados pessoais (inc. IV); implementar mecanismos para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com a Lei (inc. V); fiscalizar e aplicar sanções na hipótese de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo (inc. VI); comunicar às autoridades competentes as infrações penais das quais tiver conhecimento (inc. VII) (BRASIL, 2018).

A agência, então, possui um nível superior de competência técnica e está bem posicionada para decidir qual é o melhor sentido do texto normativo e a percepção de quais fatores representam ameaças reais ao cumprimento da lei (SUNSTEIN, 2002). Pois bem, o exercício do poder regulamentar da ANPD, como toda e qualquer entidade pública, se sujeitará à aplicação do Artigo 37, da **Constituição Federal**, devendo obedecer aos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência. Contudo, no intuito de evitar uma profunda regulamentação e intervenção na atividade econômica e livre iniciativa, o §1.º do Artigo 55-J, norteia essa atividade pela mínima intervenção. Assim, é possível afirmar o tal poder da ANPD é importante porque deverá

empregar padrões de ação que facilitem o cumprimento das normas e mantenham o espírito da lei, diante das peculiaridades de cada tecnologia.

A LGPD possui dois mecanismos repressivos de proteção aos dados pessoais. O primeiro é a responsabilização administrativa por meio de sanções aplicáveis pela autoridade nacional que é a ANPD (ações como advertência, multa, publicização da infração, bloqueio e eliminação de dados pessoais). O segundo mecanismo possível é a responsabilização civil e ressarcimento de danos, por meio da ação do Poder Judiciário (MONTEIRO, 2019).

No que diz respeito à aplicação das sanções, a Lei foi clara ao delimitar que se trata de competência exclusiva da ANPD e será realizada após procedimento administrativo, sendo assegurada a ampla defesa. Importante consideração a ser feita quanto ao tema se dá na relação da Autoridade com demais órgãos públicos sancionadores. Isso porque eventuais ilicitudes cometidas no âmbito do tratamento de dados será objeto de fiscalização e punição pela ANPD e não pelo órgão que eventualmente esteja envolvido. Exemplo disso é a previsão, nos Artigos 55-J, §2.º e 55-K, ambos da MP, da articulação complementar entre a ANPD e as entidades públicas responsáveis pela regulação de setores específicos, bem como com o Sistema Nacional de Defesa do Consumidor.

Neste sentido, o processo administrativo se torna indispensável para que ocorra a apuração do ato infracionário. O acusado passará pelo processo sancionador com o devido respeito aos princípios elencados na Constituição Federal, tais como o devido processo legal, o princípio da presunção de inocência, o direito à ampla defesa e ao contraditório, o princípio da decisão motivada e o instituto da prescrição, que constam no rol de direitos e garantias constitucionais de forma positivada e obviamente deve ser garantido na atuação da Agência.

Os direitos constitucionais definidos como **Direitos fundamentais** democráticos e individuais são de eficácia e aplicabilidade imediata, portanto, o princípio da inocência é implícito no ordenamento jurídico e é um pressuposto imediato que ocorre. Também se aplica o princípio da não autoincriminação e do direito ao silêncio, verificados no Artigo 5º da Carta Magna, pois o réu tem o direito de não se expressar em juízo ou fora dele, assim evitando sua autoincriminação.

Outrossim, o direito de defesa entra como uma medida de participação na tomada de decisões administrativas. A garantia do direito de defesa está intimamente ligada a uma pretensão repressiva e é considerada um pressuposto de eficácia do procedimento administrativo (FERREIRA, 2012). Será em torno do contraditório, articulado e compreendido em visão sistêmica, que se construirão novos significados normativos capazes de viabilizar conteúdos compatíveis com os casos concretos apresentados à Agência.

O direito de defesa se apresenta de diversas formas. Ocorre que, antes de tomar uma decisão, a Administração Pública tem o dever de ouvir o administrado antes de tomar uma decisão que o afete, sendo assim a necessidade de uma prévia audiência, com a finalidade de boa administração e de garantia do indivíduo. Sendo assim, o princípio que rege não é apenas de justiça, mas também de eficácia (FERREIRA, 2012).

Este princípio se assenta na necessidade de o Estado ter a tutela do bem-estar dos cidadãos e atender às classes menos favorecidas da sociedade, e, portanto, deve-se fazê-lo ouvindo e fornecendo o direito às pessoas a se defender antes de tomar decisões.

Aline Menezes

Mestre em Cultura Jurídica pela Universitat de Girona (Espanha). Especialista em Direito Civil e Empresarial pela Universidade Federal de Pernambuco. Graduada em Direito pela Universidade Católica de Pernambuco. Presidente da Comissão de Direito Digital da OAB - Subseção Olinda-PE. Palestrante. Realiza pesquisas na área de proteção de dados e suas repercussões na esfera cível, visando a elaboração de projeto para Doutorado.

Marcos André Barbosa Campello

Advogado, especialista em Direito Público e Direito da Comunicação Digital, membro da Comissão de Direito da Tecnologia da Informação.

Antônio Araújo Junior

CEO da Athoncorp, uma empresa de consultoria em inovação mercadológica. Professor universitário, cientistas computacional e Palestrante de educação empreendedora, estratégias mercadológicas, tecnologia disruptivas, LGPD e alfabetização de dados. Focado na área de Direito Digital, Compliance e Cyber crimes financeiros. Escritor do Blog TaJusto.com.br. Membro da Comissão de Direito e da Tecnologia da Informação da OAB/PE.

Camila Maria de Moura Vilela

Advogada e professora, mestranda em Direito Intelectual pela Universidade de Lisboa (FDL), participação especial no Curso de Pós-graduação em Direito Intelectual (APDI), pós-graduada em Direito Público (ASCES-UNITA), membro associada à Associação Portuguesa de Direito Intelectual (APDI), cofundadora do Legal Hackers Lisboa.

Daniel Miaja Simões Guimarães
Advogado, pós-graduado em direito público pela FACESF. Membro da Comisão de Direito e Tecnologia da OAB/PE.

Referências

- BRASIL. Presidência da República. **Medida provisória nº 869, de 27 de dezembro de 2018.** Brasília, DF: Presidência da República. Disponível em: http://www.in.gov.br/materia//asset_publisher/Kujrw0TZC2Mb/content/id/57220361/do1-2018-12-28-medida-provisoria-n-869-de-27-de-dezembro-de-2018-57219992. Acesso em: 15 out. 2019.
- BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGDPD). (Redação Dada pela Lei nº 13.853, de 2019). Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 16 out. 2019.
- BRASIL. Presidência da República. **Lei nº 8.429.** Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8429.htm. Acesso em: 16 out. 2019.
- BRASIL. Presidência da República. **Lei nº 13.105, de 16 de março de 2015. Código de Processo Civil.** Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 16 out. 2019.
- CORDEIRO, Renato Sobrosa. **Prescrição Administrativa**. R. Dir. Adm., Rio de Janeiro, n. 207, jan.mar. 1997. Disponível em: http://bibliotecadigital.fgv.br/ojs/index.php/rda/article/viewFile/46940/46295. Acesso em: 14 out. 2019.
- D'URSO, Luiz Flávio Borges. **PEC dos recursos e presunção de inocência**. Revista Jurídica Visão Jurídica, São Paulo, n.64, p. 25, set. 2011.
- DELGADO, José Augusto. **Ação declaratória e medida cautelar**. R, Fac. Dit. UFG. v. 7, n.1-2, jan./dez. 1983. Disponível em: https://www.revistas.ufg.br/revfd/article/view/11424/7506. Acesso em: 15 out. 2019.
- FERRARI, Rafael. **O princípio da presunção de inocência como garantia processual penal.** Âmbito jurídico, n. 102, 2012. Disponível em: https://ambitojuridico.com.br/edicoes/revista-102/o-principio-da-presuncao-de-inocencia-como-garantia-processual-penal/. Acesso em: 14 out. 2019.
- FERREIRA, Luiz Alexandre Cruz. **O direito de defesa na concepção dos atos administrativos**. Revista jurídica, [s.l.], 2012. Disponível em: https://www.uniaraxa.edu.br/ojs/index.php/juridica/article/viewFile/84/76. Acesso em: 16 out. 2019.
- FERREIRA, Daniel. **Sanções Administrativas**.1. ed. São Paulo: Malheiros, 2001. (Coleção Temas de Direito Administrativo).
- FREITAS. Juarez. **O controle dos atos administrativos e os princípios fundamentais**. 3.ed. São Paulo: Malheiros, 1999.
- GRINOVER, Ada Pellegrini. **Do direito de defesa em inquérito administrativo.** R. Dir. adm., Rio de Janeiro, n. 183, p. 9-18, jan/mar. 1991.
- MELLO, Celso Antonio Bandeira de. **Curso de Direito Administrativo**. 33. Ed. São Paulo: Malheiros, 2018.
- MELLO, Rafael Munhoz**. Sanção administrativa e o princípio da culpabilidade**. A & C R. de Dir. Administrativo e Constitucional, Belo Horizonte, ano 5, n. 22, p. 25-57, out./dez. 2005
- MONTEIRO, Yasmim Sousa. **A efetividade dos mecanismos de proteção de dados pessoais na Lei 13.709/2018.** Trabalho de Conclusão de Curso (Graduação em Direito) – Faculdade de Ciências Jurídicas e Sociais, Centro Universitário de Brasília, Brasília, DF, 2019. Disponível em: https://repositorio.uniceub.br/jspui/bitstream/prefix/13383/1/21486829.pdf. Acesso em: 16 out. 2019.
- MORAES; Alexandre de. **Direito Constitucional.** 21. ed. São Paulo: Atlas, 2007.

- OLIVEIRA, Regis Fernandes de. Infrações e sanções administrativas. 3 ed. rev. atual. e ampliada. Recife: Editora Revista dos Tribunais, 2012.
- OSÓRIO, F. M. **Direito Administrativo Sancionador.** São Paulo: Revista dos Tribunais, 2011.
- PARACCHINI, Vanessa D'Arcangelo Ruiz. **Meios repressivos à imoralidade administrativa.** Trabalho de conclusão de curso (Graduação em Direito) – Universidade Federal do Paraná, Curitiba, 2005. Disponível em: https://www.acervodigital.ufpr.br/bitstream/handle/1884/41737/M660.pdf?sequence=1&isAllowed=y. Acesso em: 16 out. 2019.
- PINHEIRO, Patrícia P**. Proteção de dados pessoais: comentários à lei n. 13.709/2018 LGPD**. São Paulo: Saraiva Educação, 2018.
- RODRIGUES, Leonardo Schmidt Durand. **Direito administrativo sancionador e jus puniendi estatal: a diferenciação dos regimes sancionatórios e as liberdades punitivas.** Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade Federal do Estado de Santa Catarina, Florianópolis, 2014. Disponivel em: https://repositorio.ufsc.br/bitstream/handle/123456789/127576/DURAND%2C%20Leonardo%20%20Direito%20Administrativo%20Sancionador%2C%20Direito%20de%20Interven%C3%A7%C3%A3o%2C%20Administrativa%C3%A7%C3%A3o%20da%20tutela%20penal.pdf?sequence=1. Acesso em: 14 out. 2019.
- SANTOS, Sterphany de Andrade. **O princípio da motivação**. Jus, [s.l.], 2014. Disponível em: https://jus.com.br/artigos/28619/o-principio-da-motivacao. Acesso em: 14 out. 2019.
- ZANATTA, Rafael A. F. **Proteção de dados pessoais como regulação de risco: uma nova moldura teórica?** I Encontro da Rede de Pesquisa em Governança da Internet. Rio de Janeiro, 2017. p. 181-188.
- ZAVASCKI, Teori Albino. **Medidas Cautelares e Medidas Antecipatórias**: Técnicas diferentes, função constitucional semelhante. Revista Trimestral de Direito Público, n. 14, p. 35-51, 1996.

Glossário

Para consultar e aprender

Administração Direta - é o próprio ente da Federação, dos quais fazem parte, na estrutura federativa brasileira, a União, os estados, o Distrito Federal e os municípios, todos pessoas jurídicas de direito público.

Administração Indireta - são as autarquias, fundações, empresas públicas e as sociedades de economia mista.

Algoritmos - Sequência finita de ações executáveis que visam obter uma solução para um determinado tipo de problema.

Aplicativo - ***Software*** de computador ou programa, objeto de download, comumente utilizado em telefones celulares.

Autonomia informativa - é a autodeterminação informativa como o direito de acrescentar, retificar e cancelar dados pessoais constantes de banco de dados eletrônicos (privados ou públicos). Ou seja, é o princípio segundo o qual o indivíduo tem o controle sobre as suas próprias informações pessoais, decidindo quais informações poderão ou não ser reveladas, a quem serão reveladas e com que objetivo.

Autoridade Nacional de Proteção de Dados – ANPD - Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei 13.709/2018 (LGPD) em todo o território nacional.

Big data - Tecnologia não inteligente que armazena massivo volume de dados, estruturados ou não, podendo processá-los e organizá-los para inferir a (re)corrência de acontecimentos.

Bill of Rights - o termo bill, que significa projeto de lei, era o documento jurídico com normas de direito individual dos cidadãos e limitações ao poder dos governantes. O mais conhecido é o *Bill of Rights*, uma carta de direitos criada e aprovada pelo Parlamento da Inglaterra em 1689, após a Revolução Gloriosa de 1688, sendo um marco importante no avanço dos direitos individuais, reduzindo o poder do monarca e ampliando os poderes do Parlamento.

Cibercultura - Aspecto da cultura contemporânea. É o conjunto de atitudes e costumes que foram sendo desenvolvidos pelas pessoas a partir do contato com os suportes tecnológicos.

Código de Defesa do Consumidor - É um conjunto de normas de proteção e defesa do consumidor, de ordem pública e interesse social, nos termos dos Artigos 5º, inciso XXXII, 170, inciso V, da Constituição Federal e Artigo 48 de suas Disposições Transitórias.

Compartilhamento de dados - Transferência ou permissão de uso dos dados para terceiros diferentes daquele que coletou a informação.

Constituição Federal - Trata-se da lei fundamental, dotada de supremacia. A Constituição Federal resguarda a missão de organizar o Estado e a Sociedade. É o estatuto do Poder e o instrumento jurídico com que a sociedade expressa normas que garantem direitos fundamentais aos cidadãos e alguns aspectos essenciais para a convivência de pessoas e grupos sociais.

Controlador de Dados - pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. é o principal tomador das decisões que envolvem os dados pessoais coletados. Ele

determina a razão da coleta dos dados; controla como eles serão coletados e posteriormente usados; seleciona quais dados serão coletados, bem como quem terá seus dados coletados; define quanto tempo esses dados permanecerão armazenados; e estabelece quem terá acesso a esses dados.

Dados anonimizados - Trata-se de dados, informações originariamente relativas a uma pessoa, mas que não são passíveis de identificá-la, eis que através de processamento técnico deixa de ser possível a identificação da pessoa. São dados essenciais para o crescimento da inteligência artificial

Dados pessoais - Referem-se a toda informação relacionada a um indivíduo, identificado ou identificável. Um conjunto de informações distintas que podem levar à identificação de uma determinada pessoa.

Dados sensíveis - Qualquer dado pessoal que revele a orientação religiosa, política ou sexual, a convicção filosófica, a procedência nacional, a origem racial ou étnica, a participação em movimentos políticos ou sociais, informações de saúde, genéticas ou biométrica do titular dos dados

Design thinking - é um conjunto de ideias práticas e criativas que visa a resolução de problemáticas em diversas áreas, agindo com base na coletividade colaborativa do desenvolvimento desses projetos, buscando encontrar respostas revolucionárias ou inovadoras para os problemas identificados.

Direitos da personalidade - São direitos imprescindíveis que constituem a manifestação da personalidade do próprio sujeito, são inerentes e essenciais a ele e garantem à pessoa o respeito e livre uso do próprio ser em todo tipo de manifestação e aspectos constitutivos de sua identidade

Direitos fundamentais - São direitos previstos na Constituição Federal, inerentes à pessoa humana enquanto indivíduos de direito e essenciais à vida digna.

Economia criativa - Refere-se ao conjunto de atividades econômicas, que utilizam a criatividade dos indivíduos como matéria-prima para geração e distribuição de bens e serviços.

Fórum Econômico Mundial - Organização sem fins lucrativos baseada em Genebra, é mais conhecido por suas reuniões anuais em Davos, Suíça nas quais reúne os principais líderes empresariais e políticos, assim como intelectuais e jornalistas selecionados para discutir as questões mais urgentes enfrentadas mundialmente, incluindo saúde e meio-ambiente.

GDPR - General Data Protection Regulation - Tradução em inglês da Regulamentação Geral de Proteção de Dados 2016/679 - RGPD, que consiste em uma lei que visa garantir a privacidade e a segurança dos dados pessoais nos países da União Europeia.

Inteligência artificial - Inteligência similar à humana exibida por mecanismos ou software, além de também ser um campo de estudo acadêmico.

ISO - Organização Internacional de Padronização, popularmente conhecida como ISO (em inglês: *International Organization for Standardization*), é uma organização internacional que cria padrões/normas para cada tipo de indústria, visando uma melhor coordenação e união internacional. Atualmente 164 países fazem parte da ISO.

Lei de Acesso à Informação - Lei nº 12.527/2011, conhecida como Lei de Acesso à Informação - LAI, regulamenta o direito, previsto na Constituição, de qualquer pessoa solicitar e receber dos órgãos e entidades públicos, de todos os entes e Poderes, informações públicas por eles produzidas ou custodiadas.

Lei Geral de Proteção de Dados Pessoais - Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de

liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

m-Saúde - tecnologia aplicada à área de saúde

Machine Learning - É uma derivação da Inteligência Artificial (IA) que fornece aos sistemas a habilidade de, automaticamente, aprender e aprimorar a partir da experiência, sem a necessidade de uma programação expressa.

Mercado *tech* - Segmento da economia em que são negociados a venda de bens e prestação de serviços tecnológicos. A exemplo: serviços de *Web Design*, de manutenção e suporte; vendas de aparelhos eletrônicos e software.

Mundo digital - Expressão utilizada para ilustrar a crescente digitalização das relações, sejam elas jurídicas ou não.

Política de privacidade - Conjunto de termos, que possui a finalidade de informar ao usuário seus direitos, garantias, formas de uso, dados recolhidos e as práticas adotadas quanto a estes, esclarecendo seu processamento e descarte. Além de informar ao usuário o que será feito com seus dados, pode também isentar o provedor de qualquer responsabilidade decorrente da falta de consentimento.

Privacidade - Faculdade que tem cada indivíduo de obstar a intromissão de estranhos em sua vida privada e familiar, assim como de impedir-lhes o acesso a informações sobre a privacidade de cada um, e impedir que sejam divulgadas informações sobre esta área de manifestação existencial do ser humano

Privacy by default - É a ideia pela qual, um produto ou serviço, em regra, deve ser lançado no mercado com as configurações de privacidade no modo mais restrito possível (por padrão), e o usuário deve ter a liberdade de permitir o acesso à coleta de mais informações caso julgue necessário.

Privacy by design - É um conceito que incorpora valores de segurança, ética e transparência no processo de desenvolvimento de projetos, produtos e serviços que trazem a privacidade desde a concepção.

Revolução Digital - A Revolução Digital, também conhecida como a Terceira Revolução Industrial, refere-se aos processos associados à passagem da tecnologia eletrônica, mecânica e analógica para a eletrônica digital, iniciada entre o final dos anos 1950 e o final dos anos 1970, com expansão do uso de computadores digitais e a constituição de arquivos digitais, processo que segue até os dias atuais. (SCHOENHERR, Steven E. San Diego, 2004).

Rol taxativo - Lista determinada e limitada, normalmente constante em um artigo de lei, que não possibilita interpretações extensivas.

Sanção - Poderá se referir ao ato de aprovação de algo por vias formais, como também, dependendo do contexto, poderá ser enquadrada como a punição pela violação de uma lei.

Segurança de dados - É a proteção de dados contra acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. A segurança de dados busca proteger a confidencialidade, a integridade, a disponibilidade e a privacidade dos dados e informações.

Sociedade de Economia Mista - É uma pessoa jurídica, cuja criação é autorizada por lei, como um instrumento de ação do Estado, dotada de personalidade de Direito Privado, mas submetida a certas regras especiais, decorrentes desta sua natureza auxiliar da atuação governamental, constituída sob a forma de sociedade anônima, cujas ações com direito a voto pertencem em sua maioria à União ou entidade de sua **Administração Indireta**, sobre remanescente acionário de propriedade particular (MELLO, Celso Antônio Bandeira de. Curso de direito administrativo, p. 195).

Software - é uma sequência de instruções escritas para serem interpretadas por um computador com o objetivo de executar tarefas específicas. Também pode ser definido como os programas que comandam o funcionamento de um computador.

Startups - são empresas emergentes que têm como objetivo desenvolver ou aprimorar um modelo de negócio, preferencialmente escalável e repetível, dentro de um cenário de incertezas e soluções a serem desenvolvidas. Embora não se limite apenas a negócios digitais, uma startup necessita de inovação para não ser considerada uma empresa de modelo tradicional. ainda em fase de desenvolvimento que é normalmente de base tecnológica.

Termos e condições de uso - Contrato de adesão, de cunho genérico, normalmente utilizado em negócios jurídicos realizados de forma online, prevendo as regras estabelecidas para aquele contrato.

Titulares dos dados pessoais - Conforme o artigo 5°, inciso V da LGPD, titular é toda pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

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.

Tratamento automatizado - Tratamento de dados sem intervenção direta do humano.

Usuários da internet - Usuário é a pessoa física ou jurídica que acessou, utilizou a internet no mínimo uma vez nos últimos três meses.

Vacatio legis – Deriva do latim e significa que há uma vacância da lei, o seja, corresponde ao período entre a data da publicação e o início da vigência de uma lei. Serve para a sociedade se adaptar a uma lei antes dela entrar em vigor.

Vazamento de dados - Transmissão não autorizada de dados para um destino ou destinatário externo.

WhatsApp - é um aplicativo multiplataforma de mensagens instantâneas e chamadas de voz para smartphones. Além de mensagens de texto, os usuários podem enviar imagens, vídeos e documentos em PDF, além de fazer ligações grátis por meio de uma conexão com a internet.