Curso – Lei Geral de Proteção de Dados

1.1. Legislações de privacidade e proteção de dados (panorama histórico internacional e nacional).

Para entendermos melhor a Lei Geral de Proteção de Dados, é imprescindível que saibamos qual é a história da proteção de dados.

Pelos registros históricos, podemos observar que em 1890 dois advogados dos Estados Unidos, Samuel D. Warren e Louis Brandeis, escreveram o artigo "O direito à privacidade", um artigo que refere sobre "o direito de ser deixado em paz", usando essa frase como uma definição de privacidade.

No ano de 1948 a Declaração Universal dos Direitos Humanos, adotada pela Assembleia Geral da ONU, estabeleceu as fundações de liberdade, justiça e paz mundiais, elencando os direitos inalienáveis de todos os membros da raça humana. Reconheceu, também, os valores de proteção da privacidade individual e familiar (art. 12) e a liberdade de informação, opinião e de expressão (art. 19). É, portanto, sem dúvidas, a matriz de inspiração de todas as leis protetivas de dados pessoais.

Em 1967 a Lei da Liberdade de Informação (FOIA) entra em vigor nos EUA e dá a todos o direito de solicitar acesso a documentos de agências estatais, o que leva outros países a seguir o exemplo.

A Suécia, por sua vez, foi o primeiro país do mundo a aprovar uma lei nacional de proteção de dados, em 11 de maio de 1973, em resposta às preocupações públicas em torno do crescente uso de computadores para processar e armazenar dados pessoais.

Ainda em 1973 e 1974 o Conselho da Europa editou as Resoluções 22 (1973) e 23 (1974), para estabelecer princípios para a proteção de informações pessoais em banco de dados automatizados, tanto no setor público, como no privado.

Em 1979 oito membros da Comunidade Europeia passaram a implementar leis nacionais de privacidade, sendo eles Dinamarca, França, Alemanha, Luxemburgo, Noruega, Áustria, Espanha e Suécia. Tais países incorporaram a proteção de dados ao texto constitucional ou editaram leis com status constitucional.

Em 1980 a OCDE emitiu diretrizes sobre proteção da privacidade e fluxos transfronteiriços de dados pessoais: tais diretrizes, apesar de serem recomendações, constituíram passo importante na direção da harmonização das legislações nacionais (dos membros e dos países interessados em ingressar na Organização) de proteção de dados e fluxo internacional de dados.

Em 1981 o Conselho da Europa, na tentativa de consolidar as normativas 73/22 e 74/29, propôs a Convenção 108 para a proteção de indivíduos com relação ao processamento automático de dados pessoais, resultando no primeiro instrumento internacional que disciplina especificamente essa temática com força legal, aberto a membros e não membros da comunidade europeia.

Em 1995 observou-se que a Convenção nº 108 não compreendia todos os aspectos necessários para uma ampla e densa disciplina de proteção da privacidade, o que levou a Comissão Europeia, provocada pelo seu parlamento europeu, a editar um novo documento. A Diretiva 95/46 foi, por mais de 20 anos, o principal documento internacional sobre o assunto.

Em 2009 a União Europeia realizou uma consulta pública sobre proteção de dados pessoais, oportunidade em que recebeu 168 respostas sobre o que seria decisivo para colocar a UE no caminho de uma reforma da Diretiva 95/46.

Em 2014 uma decisão da Corte de Justiça da União Europeia concluiu que o direito europeu dá às pessoas o direito de solicitar que mecanismos de pesquisa como o Google removam resultados de consultas que incluam seu nome. O conceito se torna conhecido como “o direito de ser esquecido”.

Em 2016 a GDPR é aprovada pelo parlamento Europeu após 4 (quatro) anos de discussões, entrando em vigor em 25/05/2018. Com texto extenso e uma

preocupação notável em abranger as mais diversas possibilidades de transações envolvendo dados, a GDPR sagrou-se um marco na proteção de dados e da proteção à privacidade do usuário. Instituiu princípios sólidos e claros, a fim de não abrir margem para interpretações diversas.

O Regulamento Europeu criou no indivíduo a possibilidade de domínio sobre os próprios dados, reclamando a propriedade destes como algo pessoal e não comercial, pertencentes às empresas ou explorado pelo Poder Público.

Voltando os olhos para o Brasil, antes de ser aprovada a Lei Geral de Proteção de Dados – LGPD, o tema de proteção de dados e privacidade era tratado somente por legislações setoriais, como, por exemplo, Código de Defesa do Consumidor, Lei do Cadastro Positivo, Lei de Acesso à Informação, alguns dispositivos do Código Civil, Lei de Propriedade Industrial, Lei de Direitos Autorais, Lei do Software e Marco Civil da Internet.

1.2. O advento da Lei 13.709/2018 – Lei Geral de Proteção de Dados.

O Brasil, olhando o panorama Europeu sobre proteção de dados, observou que a GDPR havia sido aprovada, fato esse que impulsionou o Congresso Nacional a aprovar a LGPD.

O caminho até a aprovação da LGPD não foi fácil. No fim de maio do ano de 2018, a Câmara dos Deputados aprovou o seu PL nº 4.060, de modo a incorporar a redação do PL nº 5.276/2016, em regime de urgência regimental. Dessa forma, cabia, então, somente ao Senado Federal realizar a votação e aprovação do Projeto de Lei.

Ocorre, contudo, que, no âmbito do Senado, havia um Projeto de Lei (330/2013) que também versava sobre a matéria de proteção de dados e já se encontrava na Comissão de Assuntos Econômicos (CAE). Assim, com o projeto advindo da Câmara dos Deputados, houve a saída de pauta do PL (330/2013), o qual restou apensado ao projeto da Câmara (4.060/2012), o que culminou no Projeto de Lei da Câmara nº 53/2018, que somente aguardava a votação no Senado.

Em 10 de julho do ano de 2018 o Senado votou e aprovou o Projeto nº 53/2018. O então presidente Michel Temer sancionou parcialmente a Lei Geral de Proteção de Dados, constando alguns vetos em relação à criação da Autoridade Nacional de Proteção de Dados, haja vista a alegação do vício de iniciativa – falta de competência do Poder Legislativo para criar um órgão de natureza especial, com vinculação ao Ministério da Justiça, com independência administrativa, ausência de subordinação hierárquica e autonomia financeira.

Dessa forma, em relação aos vetos, restou editada a Medida Provisória nº 869/2018, a qual criou a Autoridade Nacional de Proteção de Dados e restou, posteriormente, convertida na Lei nº 13.853 de 2019.

Cabe salientar, ainda, que a MP nº 869 alterou o prazo de vacância da LGPD para 24 meses, ou seja, a Lei Geral de Proteção de Dados somente entrará em vigor em 14 de agosto de 2020.

1.3. Aplicabilidade.

A aplicabilidade da LGPD resume-se a quem ela se aplica, se a pessoas físicas ou jurídicas, bem como a sua abrangência territorial e extraterritorial.

Assim refere o artigo 1º da LGPD:

> Art. 1º Esta Lei 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.

Diante da leitura do artigo primeiro acima, é possível concluir que a LGPD preocupa-se somente com o tratamento de dados pessoais, não atingindo, portanto, dados de pessoas jurídicas, documentos confidenciais, eventuais segredos de negócios, algoritmos, patentes e outras informações as quais não sejam estritamente relacionadas às pessoas naturais identificadas ou identificáveis.

Repita-se, somente dados pessoais estão protegidos pela Lei Geral de Proteção de Dados, motivos pelo qual a análise da aplicabilidade da Lei, conforme lembra o professor Rony Vainzof[1], deverá se aprofundar no mapeamento e inventário de dados pessoais estruturados[2] e não estruturados[3].

Ademais, é de ser destacado que a nossa sociedade é, de fato, tecnológica e digital. Contudo a LGPD não só se aplica a esse mundo digital, mas, também, aos dados que estão em estado físico/*off-line*.

Por sua vez, acerca da aplicabilidade da Lei, o Artigo 3º da LGPD refere:

> Art. 3º Esta 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, desde que:
> I - a operação de tratamento seja realizada no território nacional;
> II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (Redação dada pela Lei nº 13.853, de 2019)
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
> § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.
> § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

A LGPD aplica-se, portanto, a pessoas físicas e jurídicas, de direito público ou privado, que tratem dados pessoais, independentemente do meio, do país de sua sede ou do país em que estejam localizados os dados. Diante do texto normativo, é possível concluir que a Lei somente não se aplica às pessoas físicas que realizam tratamento de dados para fins exclusivos e não econômicos.

---

[1] VAINZOF, Rony. LGPD: Lei Geral de Proteção de Dados comentada. Coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. São Paulo: Thomson Reuters. 2019, p 20.
[2] Dados existentes em banco de dados relacionais, que podem ser recuperados e processados de forma eficiente, pois organizados, como os contidos em planilhas.
[3] Dados pessoais de difícil indexação, acesso, recuperação e processamento, pois não organizados. Eles podem estar dentro de vídeos, e-mails, imagens e áudios, por exemplo.

A Lei não dá importância para a finalidade em que as organizações são constituídas. Realizado o cadastro (CNPJ) da empresa, esta adquirindo, portanto, personalidade jurídica, ela deverá realizar o cumprimento integral da LGPD caso realize tratamento de dados pessoais.

As pessoas naturais (físicas) que empregarem seus esforços necessários para o estabelecimento do seu negócio, de acordo com critérios avaliativos da responsabilidade de cada um no eventual tratamento ilícito de dados, poderão ser fiscalizadas, sancionadas e responsabilizadas.

Como é previsto na própria Lei, ela aplica-se, também, ao setor público, devendo o tratamento buscar a finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

Por fim, é importante destacar que a aplicação da LGPD também independe do país da sede ou do país da localização dos dados tratados, ampliando, assim, de forma considerável, a sua jurisdição.

No que versa a aplicação territorial e extraterritorial da LGPD, há uma imprecisão técnica na redação. Vejamos:

No inciso I, do art. 3º, o qual deveria prestar atenção apenas em estabelecimentos que tratem dados pessoais no território nacional, ou seja, dispor sobre a aplicação territorial da LGPD, ao prever a aplicação quando houver "**operação de tratamento**", em razão da amplitude desse conceito, acaba gerando, também, o dever de cumprimento da Lei aos agentes estrangeiros, mesmo sem sede no Brasil e que de qualquer forma "operem" dados pessoais no Brasil, o que inclui, por exemplo, a mera coleta, produção ou recepção dos dados pessoais.

Para melhor ilustrar a questão, uma empresa com sede no Brasil desenvolveu um aplicativo *mobile* de entrega de comida para usuários na Austrália e no Japão, somente disponibilizando o serviço para esses dois países, de forma a coletar

dados somente internacionalmente, sem quaisquer dados coletados de brasileiros. Tendo em vista que as atividades de coleta e processamento de dados são realizadas pelo controlador, situado no Brasil (território nacional), aplica-se a ele a LGPD.

A regra é clara, basta a existência da operação de tratamento de dados pessoais em território nacional para que a LGPD seja aplicada.

O inciso II, do art. 3º, por sua vez, prevê a aplicação extraterritorial da LGPD, ou seja, em quais momentos a Lei aplica-se a indivíduos estrangeiros. Assim, se a atividade de tratamento tiver por objetivo a oferta ou fornecimento de bens ou o tratamento de dados de indivíduos localizados no território nacional, independentemente da localização geográfica do controlador.

O professor Rony Vainzof[4] explica que:

> "Quando agentes de tratamento estrangeiros visam prover serviços e explorar outro mercado, a partir do momento em que determinado mercado ganha corpo econômico, é cogente que se avalie as regras locais a que estarão sujeitos. É o conceito de direcionamento (*targeting criterion*) de bens ou serviços ou do foco no tratamento de dados para indivíduos, no caso, localizados no território nacional, mesmo sem a existência de um integrante do grupo econômico no Brasil, conforme inclusive já era previsto no Marco Civil da Internet, ao dispor sobre a aplicação da legislação brasileira para dados coletados em território nacional, mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil."

Portanto, **independentemente da sede física do responsável pela atividade de tratamento de dados, considerando que eventuais lesões aos titulares terão reflexo no Brasil, diante do foco do produto ou serviço ser o mercado brasileiro ou o tratamento de dados de indivíduos no Brasil, a LGPD deverá ser cumprida**.

[4] VAINZOF, Rony. LGPD: Lei Geral de Proteção de Dados comentada. Coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. São Paulo: Thomson Reuters. 2019, p. 59/60.

Cabe, ainda, salientar que a oferta ou o fornecimento de bens e serviços deverão ser realizados para os titulares que se encontram fisicamente dentro do território brasileiro, mesmo que não haja cobrança pecuniária para o serviço. É preciso identificar a intenção efetiva de se oferecer bens ou serviços a pessoas que se encontrem fisicamente no território brasileiro, ou, ainda, identificar o foco em tratar dados de titulares em território nacional.

Para ilustrar, se houver um *website* do controlador, operador ou intermediário, na internet, e, portanto, acessível aos cidadãos brasileiros, ainda que em língua portuguesa, não é suficiente para determinar a intenção prevista na LGPD para a incidência do critério previsto no inciso II.

Sobre o ponto em debate, oportuno trazer a Consideranda 23, do GDPR, a qual dispõe de alguns fatores mais objetivos que podem ensejar sua aplicabilidade de acordo com a discussão do inciso em questão: (a) ***uso de uma moeda de uso corrente do país-alvo***; (b) ***possibilidade de encomendar bens ou serviços naquela localidade***; (c) ***referência a clientes ou usuários que se encontrem naquela região, que possam ser reveladores da intenção de oferecer bens ou serviços a titulares de dados na região***.

O inciso III, do art. 3º, prevê a aplicação da Lei quando "os dados pessoais objeto do tratamento tenham sido coletados no território nacional". Ou seja, a LGPD não se importa se o controlador ou o operador tiver como objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de pessoas localizadas no Brasil, de modo que a mera coleta de dados pessoais basta para incidência da Lei.

O já citado professor Rony Vainzof[5] refere que:

> "primeiramente houve atecnia do inciso primeiro ao não delimitar a aplicação da Lei ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento do agente do tratamento situado no Brasil, mas sim prever o cumprimento da Lei em qualquer "operação de tratamento realizada

[5] VAINZOF, Rony. LGPD: Lei Geral de Proteção de Dados comentada. Coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. São Paulo: Thomson Reuters. 2019, p 63.

> em território nacional", culminando na abrangência, também, quando dados pessoais são somente coletados no Brasil."

Diante dessa situação, a melhor saída para o legislador seria corrigir o inciso I, de modo a deixar clara a aplicação territorial somente no "critério do estabelecimento" e eliminar o inciso III, pois, assim, a aplicação extraterritorial se daria não meramente da coleta de qualquer dado pessoal em território nacional, mas, sim, nos casos dos testes anteriormente citados.

Essa questão é de suma importância, pois, se não forem analisados e modificados os critérios de aplicabilidade, poderá, sem dúvidas, impactar na possibilidade de novos serviços serem disponibilizados no país. Isso porque, se as organizações internacionais tomarem conhecimento de que um mero acesso oriundo do Brasil pode implicar a elas o dever de cumprimento e, consequentemente, as sanções previstas na LGPD, certamente visarão o bloqueio do país.

Essa referida falta de técnica na redação dos incisos ora comentados deverá ser solucionada pela Autoridade Nacional de Proteção de Dados que possui alçada para interpretar a LGPD, de modo a realizar uma mitigação dessa atecnia.

Exceções de aplicabilidade da LGPD estão previstas no art. 4º. Vejamos:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
> II - realizado para fins exclusivamente:
> a) jornalísticos e artísticos; ou
> b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
> III - realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> d) atividades de investigação e repressão de infrações penais; ou
> IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país

> que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.
> § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.
> § 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.
> § 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público.

- **I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;**

A exceção prevista no inciso I do art. 4º é importante para que a incidência da LGPD esteja direcionada para questões que realmente possam pôr em risco a privacidade e os direitos da personalidade dos seus titulares.

Assim, as atividades pessoais, como, por exemplo, as domésticas, correspondências, endereços, atividades em redes sociais, rede *wi-fi* doméstica, encontram respaldo na exceção ora analisada.

Caso diferente seria o das gravações decorrentes de câmeras de monitoramento internas (dentro da residência da pessoa física) e externas (espaço público), por contemplarem as imagens (como rosto) de terceiros, que são armazenadas em nuvem e em dispositivos pessoais dos donos da residência, por exemplo, aplicar-se-ia a LGPD, tanto para a empresa de armazenamento em nuvem como para o dono da residência, principalmente em razão da possibilidade de captação de uma quantidade grande de imagens de terceiros.

Assim, a exceção em referência deve ser analisada de forma limitativa, sopesando o risco aos direitos dos titulares dos dados.

- **II - realizado para fins exclusivamente: a) jornalísticos e artísticos; ou**

A exceção ora vista visa à proteção do jornalismo. Contudo, não concede uma isenção geral da Lei para as mídias e entidades que processem dados pessoais. Importante salientar que qualquer informação relacionada à pessoa natural identificada ou identificável (art. 5º, I) é considerada dado pessoal, mesmo que o acesso seja público, de forma que o tratamento desses dados deverá observar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

Assim, entidades que eventualmente busquem se enquadrar nessa exceção, devem ser cautelosos ao separar as diversas bases de dados, de acordo com as respectivas finalidades, pois deverão demonstrar à ANPD que determinados dados são utilizados exclusivamente para fins jornalísticos, a fim de aplicar a exceção sobre eles.

- **II - realizado para fins exclusivamente: b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;**

A exceção prevista para os fins acadêmicos deverá observar as mesmas pontuações feitas à exceção anterior, principalmente a cautela na publicação de trabalho científico, de modo a sopesar o interesse público e os direitos dos titulares.

Ainda, conforme prevê o art. 7º, IV, e o art. 11, II, "c", sempre que possível deverá buscar-se meios técnicos razoáveis e disponíveis no momento do tratamento, pelos quais o dado perde a possibilidade de associação, direta ou indireta, a um indivíduo (anonimização), ou realizar o tratamento por meio do qual o dado perde a possibilidade de associação direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro (pseudominização).

- **III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; ou**

O legislador andou bem em vez de criar um grande marco legal que também pudesse versar sobre hipóteses legais que autorizariam o tratamento de dados pessoais para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações legais, ter excepcionado a aplicação da LGPD para as finalidades acima listadas, diante da necessidade de um amadurecimento na eventual necessidade de alteração das legislações já em vigência que autorizam e limitam o tratamento de dados pessoais, sopesando segurança e privacidade.

- **IV – provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.**

A exceção acima visa a, de alguma forma, estimular a economia brasileira, tornando o Brasil um território receptivo e sem entraves burocráticos, no que se refere à proteção de dados pessoais, para organizações estrangeiras que queiram armazenar dados no país, seja mediante o estabelecimento de uma filial em território nacional, seja mediante a contratação de uma empresa nacional para a finalidade.

A lei dispõe dos seguintes requisitos, os quais devem ser cumulados:

(i) Dados oriundos de país estrangeiro. Portanto, não podem ser coletados em território nacional;

(ii) Não pode haver comunicação ou uso compartilhado de dados com agentes brasileiros. Portanto, a operação pode incluir a recepção, classificação, processamento, arquivamento, armazenamento e eliminação de dados pessoais, do que se extrai que esse tratamento específico somente poderia ser realizado por operador, pois, como controlador, o agente tomaria decisões sobre o tratamento que poderiam fulminar a exceção;

(iii) Também não pode haver transferência internacional de dados com outro país que não o de proveniência. Portanto, caso uma empresa multinacional queira se beneficiar do Brasil por meio dessa exceção, os dados somente poderão transitar entre o país de origem e o Brasil, cessando a exceção caso outra filial, sediada em outra nação, receba os dados localizados em território nacional;

(iv) Por fim, o país de proveniência deve ter grau de proteção de dados pessoais adequado ao previsto na LGPD, motivo pelo qual a exceção em questão é de eficácia contida, vez que o nível de proteção de dados do país estrangeiro será avaliado e chancelado pela ANPD.

Esses requisitos pretendem aumentar a competitividade internacional brasileira, estimulando a contratação de empresas nacionais para serviços de tecnologia da informação, como *hosting* tradicional ou em nuvem, IT *Outsourcing*, *analytics*, entre outros, sem que o Brasil se transforme em um "paraíso de dados".

1.4. Conceitos importantes.

O art. 5º da LGPD lista uma série de conceitos importantes para que possamos melhor compreender e aplicar a legislação.

Artigo 5º. Para os fins desta Lei, considera-se:

I – Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

O Brasil, com a LGPD, adota o conceito expansionista de dado pessoal, pelo qual não somente a informação relativa à pessoa diretamente identificada estará

protegida pela Lei, mas, também, aquela informação que possa – tem o potencial de – tornar a pessoa identificável[6].

Assim, nome, sobrenome, RG, CPF, título de eleitor, número de passaporte, endereço, estado civil, gênero, profissão, origem social e étnica; informações relativas à saúde, à genética, à orientação sexual, às convicções políticas, religiosas e filosóficas; número de telefone, registro de ligações, protocolos de internet, registros de conexão, registro de acesso a aplicações de internet, contas de e-mail, cookies, hábitos, gostos e interesses, são apenas alguns exemplos de dados pessoais que pautam a atual vida em sociedade.

A Lei, como já anteriormente referido, tutela somente "dados pessoais", o que implica que o dado esteja intrinsicamente vinculado a uma pessoa natural identificada ou identificável. Conforme dispõe o professor Danilo Doneda, é importante distinguir dados gerais de dados pessoais, pois estes últimos possuem um vínculo objetivo com a pessoa, justamente por revelar aspectos que lhe dizem respeito.

Assim, torna-se imperioso, seja direta ou indiretamente, ter o componente da identidade de uma pessoa natural como característica fundamental do dado pessoal.

Quando conectados à esfera de uma pessoa natural, a proteção de dados significa um resguarda da própria personalidade do ser humano, haja vista que esta constitui "as características que distinguem uma pessoa", e o direito visa a proteger violações de todos os atributos, sejam corpóreos e incorpóreos, que formam a projeção da pessoa.

Portanto, podemos classificar os dados, de acordo com a LGPD, da seguinte forma:

[6] VAINZOF, Rony. LGPD: Lei Geral de Proteção de Dados comentada. Coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. São Paulo: Thomson Reuters. 2019.

- Dados pessoais **diretos**: identifica diretamente uma pessoa natural, sem a necessidade de outras informações, como CPF, RG, título eleitoral, nome (se não houver homônimos);

- Dados pessoais **indiretos**: torna a pessoa natural identificável, pois necessitam de informações adicionais para identificá-la, como gostos, interesses, hábitos de consumo, profissão, sexo, idade e geolocalização.

II – Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Em termos gerais, os dados pessoais sensíveis são dados pessoais que podem, de alguma forma, trazer algum tipo de discriminação quando do seu tratamento. Ou seja, são dados pessoais que podem implicar riscos e vulnerabilidades potencialmente mais gravosas aos direitos e liberdades fundamentais dos titulares.

Tal categoria especial de dados pessoais é fruto de uma observação da diferença que apresenta o efeito do tratamento desses tipos de dados em relação aos demais. Diante disso, a LGPD dedica obrigações diferenciadas ao tratamento dos dados pessoais sensíveis. Vejamos:

- As bases legais para o tratamento de dados pessoais sensíveis são diferenciadas e limitadas, dispostas no art. 11 da LGPD;
- Quando a base legal para o tratamento for o consentimento, além de ser livre, inequívoco e informado, também deverá ser específico e destacado;
- Não há base legal para o tratamento de dados sensíveis por interesse legítimo;
- Não há base legal para o tratamento de dados sensíveis para a proteção do crédito;

- Da mesma forma, não há base legal para o tratamento de dado sensível para a execução de contrato ou procedimentos preliminares relacionados a contrato, mas sim para o exercício regular de direitos, inclusive em contrato.

Os controladores deverão avaliar situações com precisão, haja vista que dados pessoais tratados em larga escala, ainda mais de forma automatizada, poderão resultar no processamento de dados pessoais sensíveis.

Exemplo a ser dado é quando da análise da geolocalização em uma aplicação (Uber) se consiga traçar eventual comportamento do titular de modo que se possa inferir se o titular possui alguma doença específica, em razão da quantidade de vezes que o titular vai a algum hospital específico.

A ONG *article 19*, em seu trabalho *Privacy and freedom of expression in the age of artificial intelligence*, concluiu que os métodos de Inteligência Artificial estão sendo utilizados para identificar pessoas que desejam permanecer anônimas; inferir e gerar informações sensíveis sobre pessoas a partir de seus dados não sensíveis; criar perfis de pessoas com base em dados em escala populacional; e tomar decisões subjacentes utilizando esses dados, alguns dos quais podem afetar profundamente a vida das pessoas.

Por fim, para melhor compreensão da abrangência de alguns dos dados sensíveis previstos na LGPD, o GDPR serve, mais uma vez, como ótimo parâmetro:

- **Dados referentes à saúde**: relacionados com a saúde física ou mental de uma pessoa, incluindo aqueles relativos à prestação de serviços médicos, que revelem informações sobre o seu estado de saúde. Por exemplo, a quantidade de passos diários coletados de um indivíduo, por si só, não necessariamente será um dado sensível, mas, dependendo da tecnologia empregada, pode ser um indicativo de sedentarismo, transformando-se em um dado sensível;
- **Dados genéticos**: relativos às características genéticas, hereditárias ou adquiridas de uma pessoa que tragam informações únicas sobre a sua fisiologia ou saúde e que resulte de uma análise de uma amostra biológica proveniente da respectiva pessoa;

- **Dados biométricos**: resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa que permitam ou confirmem a identificação única dessa pessoa, notadamente imagens faciais ou dados dactiloscópicos. Porém, fotografias não deverão ser consideradas automaticamente dados sensíveis, pois necessitam da avaliação se o processamento se deu por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação da pessoa[7].

III – Dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

Vamos tratar aqui tanto o conceito de "dado anonimizado" como de "anonimização", para maior precisão e compreensão dos institutos.

Conforme já referido, a LGPD não considera dado anonimizado, ou seja, dado relativo a titular que não possa ser identificado, como sendo dado pessoal, o que resulta na inaplicabilidade da legislação em estudo para tal tipo de dado.

Assim, da mesma forma, os dados que passaram por procedimento de "anonimização", que é a utilização dos meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação direta ou indireta, a um indivíduo, também perdem a incidência da LGPD.

Essas premissas são extremamente pertinentes, haja vista que o objetivo da Lei é tutelar os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Nesse sentido, quando o dado não tiver condições de identificar ou tornar identificável determinada pessoa natural, o mesmo não possui razão de ser protegido pela Lei.

Contudo, vale mencionar que "dado anonimizado" e "anonimização" não se confundem com "pseudonimização de dados", que ocorre quando um dado perde a

[7] Consideranda 51 do GDPR.

possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro. Nesse caso, o dado permanece pessoal.

A Lei elenca alguns critérios para avaliação de que o dado esteja anonimizado, seja no momento do seu tratamento ou após o processo de anonimização. Vejamos:

- Impossibilidade de o titular ser identificado ou perda de possibilidade da associação, direta ou indireta, do indivíduo;
- Mediante a utilização de meio técnico razoável e disponível na ocasião de seu tratamento;
- O processo de anonimização não pode ser revertido, com utilização exclusiva de meios próprios ou por esforços razoáveis;
- O esforço razoável será determinado com base em fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização de meios próprios.

No trabalho acadêmico *Facial recognition systems and their data protection risks under the General Data Protection Regulation* são expostas algumas situações de dados anonimizados:

Padrões de imagem ou as características extraídas dos indivíduos, em particular, utilizadas somente para categorização (ex. referente a gênero, idade, etnia, vestuário) não serão considerados dados pessoais. Para exemplificar, quando uma única imagem de vídeo é capturada e a única informação armazenada se refere a estas estatísticas, é improvável que os dados sejam capazes de identificar qualquer pessoa ou possibilitar resultados precisos ou confiáveis.

IV – Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou vários locais, em suporte eletrônico ou físico;

O conceito de banco de dados se resume à estruturação conjunta de dados que identifiquem ou possam identificar uma pessoa natural. A proteção da Lei seguirá o conjunto estruturado de dados pessoais em qualquer formato.

A bem da verdade, o conceito de banco de dados é previsto na LGPD a fim de facilitação das medidas práticas de bloqueio ou de eliminação. Assim, na aplicação dessas medidas, elas devem se restringir aos dados pessoais contidos nos bancos de dados.

V – Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

O titular de dados é o núcleo duro da existência da Lei, haja vista que a preocupação sobre eventuais violações aos direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade está diretamente vinculada à pessoa natural.

VI – Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII – Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

Visando a facilitar o entendimento das obrigações e responsabilidades, serão tratados conjuntamente os dois conceitos acima.

É sobre o controlador que a LGPD impõe seu maior peso jurídico, pois é ele o responsável pela tomada de decisões sobre o tratamento de dados pessoais.

É fundamental definir quem é o controlador em cada caso concreto, para que a LGPD seja devidamente cumprida na prática, afinal de contas ele que:

- Deve avaliar o enquadramento de ao menos uma das bases legais para a realização de cada tratamento de dados pessoais;

- Deve acompanhar o ciclo de vida completo dos dados, descartando-os ou determinando o descarte quando do término do tratamento;
- Deve indicar o Encarregado;
- É competente pela elaboração do relatório de impacto à proteção de dados pessoais;
- A ele que cabe o ônus da prova sobre o consentimento do titular;
- Deve cumprir os direitos dos titulares;
- Deve demonstrar a 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;
- Deve transmitir as instruções para o tratamento de dados quando resolver envolver um operador;
- Será responsabilizado civilmente, nos casos de violação à LGPD;
- Será sancionado administrativamente em razão de infrações cometidas às normas previstas na LGPD;
- Deve comunicar à ANPD e ao titular sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares;
- Deve formular e empregar regras de boas práticas e governança em proteção de dados pessoais, levando em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular;
- Deve 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;
- Deve prestar informações quando solicitadas pela ANPD.

O operador, por sua vez, é quem realiza o tratamento de dados pessoais em nome do controlador. Portanto, este não poderá tratar dados pessoais senão em virtude das determinações do controlador ou da previsão legal. Há as seguintes previsões da LGPD quanto ao operador:

- O operador também deve manter registro das operações de tratamento de dados pessoais que realize;
- Também deve demonstrar 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;
- Será responsabilizado civilmente, em razão do exercício da sua atividade de tratamento de dados pessoais, no caso de violação à LGPD;
- Responde solidariamente pelos danos causados pelo tratamento quando descumprir obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador se equipara ao controlador;
- Responde pelos danos decorrentes da violação da segurança dos dados se deixar de adotar medidas de segurança previstas na LGPD;
- Será sancionado administrativamente em razão de infrações cometidas às normas previstas na LGPD;
- Também deve formular e empregar regras de boas práticas e governança em proteção de dados pessoais, levando em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular;
- Deve, também, prestar informações quando solicitadas pela ANPD.

Assim, é de suma importância definir quem é o controlador e quem é o operador em cada caso, o que pode ser uma tarefa complexa, haja vista que a evolução da tecnologia da informação poderá gerar situações em que uma mesma pessoa jurídica será controladora e operadora.

Importante salientar que para os titulares e para a Autoridade Nacional de Proteção de Dados não poderá haver dúvidas. Por isso, o controlador deverá se identificar, com informações de contato, perante o titular dos dados, de forma facilitada, clara, adequada e ostensiva, além de prestar informações sobre tratamento dos dados, como a finalidade específica do tratamento, forma e duração e, ainda, prestar informações acerca do uso compartilhado de dados e a finalidade.

Algumas indagações poderão contribuir para a identificação do controlador: Qual o motivo de determinado tratamento de dado estar ocorrendo? Quem teve essa ideia? Quem efetivamente deu início a qualquer uma das hipóteses previstas como tratamento?

Para melhor ilustrar a questão, imagine que uma instituição financeira contrate outra entidade para realizar o armazenamento dos dados pessoais de seus clientes, dando instrução clara que a empresa contratada não poderá realizar outro tratamento senão o mero armazenamento. Mesmo que a empresa contratada tenha alguma autonomia para melhor gerenciar o armazenamento, estará vinculada para agir de acordo com as determinações da instituição financeira. Nesse cenário, a instituição financeira será a controladora, e a empresa contratada, a operadora. Vale destacar, contudo, que, caso a empresa contratada tome alguma decisão ilícita, utilizando os dados armazenados para outras finalidades, ela se tornará, também, controladora.

Quem determina o propósito do processamento é o controlador, ou seja, questões substanciais, que são essenciais para o núcleo da legalidade do processamento, são reservadas ao controlador. Assim, eventuais questões secundárias, como meios de processamento, poderão ser delegadas pelo controlador ao operador.

Na prática, o ponto fundamental para caracterizar o controlador é a sua capacidade de determinar as finalidades para as quais os dados pessoais estão sendo coletados, armazenados, utilizados, alterados e compartilhados.

Acerca do operador, é preciso analisar se é uma entidade ou pessoa física terceira ao controlador e que realize a operação de tratamento em nome dele. Essa operação pode ser restrita a uma tarefa simples, específica e limitada, ou pode atender a uma demanda mais complexa, em que importa, até mesmo, certa discricionariedade do operador em razão de sua especialização, mas sempre cumprindo estritamente as determinações do controlador.

VIII – Encarregado: pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados;

Na LGPD, a figura do Data Protection Officer (DPO) se apresenta como Encarregado. Seu papel vai muito além de atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD, como previsto no conceito em estudo, pois ele será o responsável por aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; receber comunicações da ANPD e adotar providências; orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Até disposição ao contrário da Autoridade, todos os controladores têm a obrigação legal de indicar um Encarregado. Quanto aos operadores, não há essa expressa exigência, sendo recomendável, no entanto, de acordo com a análise da criticidade das espécies de serviços providos, quanto ao tratamento de dados pessoais, nomeá-lo para conseguir atender a todas as suas obrigações, conforme analisado em tópico anterior. Caso o operador não opte por nomear um Encarregado, sugere-se fundamentar a decisão.

Após a Medida Provisória n. 869/2018, não só a pessoa física poderá ser Encarregado, mas qualquer "pessoa" indicada pelo controlador. Ou seja, não há vedação para pessoa jurídica assumir o cargo.

O ideal, na prática, é que o Encarregado não acumule funções e tenha independência, pois, para desempenhar seu papel de orientar o controlador acerca das práticas de tratamento de dados pessoais e intermediar as relações entre ele e os titulares dos dados e a Autoridade Nacional, "há de ser livre no desempenho de suas funções, sem que receba instruções ou seja destituído em razão do (adequado) exercício de suas incumbências, ainda que suas recomendações, embora legais, sejam desfavoráveis aos negócios da empresa por ele assistida".

Ademais, o Encarregado deve se envolver com todas as questões de proteção de dados, participando das reuniões de gestão da empresa, recebendo informações sobre as atividades de tratamento e interagindo com o mais alto patamar diretivo. Dessa forma, o Encarregado deve estar presente e opinar nas tomadas de decisões que impactem na proteção de dados pessoais.

X – Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

A definição de tratamento de dados pessoais, na LGPD, é extremamente abrangente, pois parte da coleta e termina em sua eliminação, englobando todas as possibilidades de manuseio de dados, independentemente do meio utilizado. Assim, o mero ato de receber, acessar, arquivar ou armazenar dados pessoais está contido dentro do conceito de tratamento.

Referida constatação de abrangência do conceito é de fundamental importância, pois o agente de tratamento, em absolutamente todas essas hipóteses, deverá manter registros de suas operações (art. 37), bem como, no caso do controlador, avaliar o cumprimento de uma das bases legais previstas na Lei, o que implica dizer que um simples dado pessoal arquivado, mesmo que não seja processado, precisará ter um fundamento previsto na Lei para estar sob a responsabilidade do agente. Se o controlador não encontrar um embasamento jurídico para manter o dado pessoal consigo (ou com o operador), deverá eliminá-lo.

Vale destacar, ainda, que a regra no ordenamento jurídico brasileiro é a do princípio da irretroatividade da lei. Ou seja, qualquer obrigação existente em nova legislação não se aplicará às situações constituídas anteriormente à sua eficácia plena, visando a manutenção da segurança, certeza e estabilidade das normas.

Assim, a LGPD não terá efeitos sobre o tratamento de dados ocorridos antes de 16 de agosto de 2020. Porém, como o conceito de tratamento abarca

absolutamente todas as hipóteses de manuseio de dados, a partir do dia da eficácia plena da Lei, os dados pessoais anteriormente existentes, se não descartados, de alguma forma estarão sob a tutela da LGPD, mesmo que permaneçam armazenados estatisticamente.

Portanto, é fundamental que os controladores realizem um mapeamento dos dados pessoais, previamente à vigência da Lei, para avaliar o enquadramento do tratamento em uma das bases legais existentes durante todo o ciclo de vida dos dados sob a sua responsabilidade. Caso não encontre uma das bases legais, deverá suprir essa lacuna ou eliminá-los.

Os conceitos previstos nos incisos XII ao XIX serão analisados em momentos próprios e oportunos.