UNIVERSIDADE FEDERAL DE JUIZ DE FORA

ANDRÉ LUIS PARMA JÚNIOR

A MODALIDADE *THIRD PARTY TRACKING* DE COLETA DE DADOS PESSOAIS NA ORDEM JURÍDICA BRASILEIRA E UNIÃO EUROPEIA

ANDRÉ LUIS PARMA JÚNIOR

A MODALIDADE *THIRD PARTY TRACKING* DE COLETA DE DADOS PESSOAIS NA ORDEM JURÍDICA BRASILEIRA E UNIÃO EUROPEIA

Artigo apresentado junto ao curso de Direito da Universidade Federal de Juiz de Fora, para conclusão do curso.
Orientado pelo Prof. Cláudio Santos.

Juiz de Fora

2017

ANDRÉ LUIS PARMA JÚNIOR

A MODALIDADE *THIRD PARTY TRACKING* DE COLETA DE DADOS PESSOAIS NA ORDEM JURÍDICA BRASILEIRA E UNIÃO EUROPEIA

Relatório final apresentado à Universidade Federal de Juiz de Fora, como parte das exigências para a obtenção do título de graduação.

Juiz de Fora, 23 de novembro de 2017.

BANCA EXAMINADORA

_____

Prof. Claudio Santos

_____

Prof. Bruno Stigert

_____

Mestranda. Kaliandra Casati

SUMÁRIO

INTRODUÇÃO

O presente artigo visa fazer uma análise da coleta de dados pessoais por terceiros e como os ordenamentos jurídicos brasileiros e europeus tratam da referida questão. Para tal, é necessária uma análise do conceito de dados pessoais e dados pessoais sensíveis de forma a delimitar o objeto a ser perseguido pelas legislações de proteção de dados pessoais.

Seguindo essa lógica o próximo ponto a ser estudado são os processos de coleta e tratamento de dados e como eles ocorrem, sendo que o presente estudo dará maior ênfase a coleta de dados por terceiros.

Passando a análise de como os ordenamentos jurídicos tratam a questão será feita, inicialmente, uma análise histórica das legislações de proteção de dados de forma a evidenciar sua origem e evolução, bem como, destacar que a ordem de criação de legislações de proteção de dados teve como vanguardistas os países tecnologicamente mais desenvolvidos.

Mas apesar de tudo destacado nessa introdução, o mais importante é destacar a importância que se deve dar a proteção de dados pessoais, tendo em vista que conforme será observado no presente artigo a própria constituição estabelece parâmetros para proteção a intimidade e vida privada, estabelecendo, inclusive, limites ao acesso ao acesso a informação.

Por fim, o artigo faz uma análise comparada dos principais projetos de lei existentes no Brasil (PL4060/2012 e PL5276/2016) e de como a União Europeia regula a proteção de dados pessoais e pessoais sensíveis da coleta por terceiros. Essa análise é realizada através dos princípios que doutrinariamente regem a proteção de dados.

O presente estudo demonstra sua importância tendo em vista que o Brasil ainda se encontra em fase de criação legislativa a respeito do respectivo tema, sendo, portanto, um tema atual e inovador no ordenamento nacional.

1.DADOS PESSOAIS, O QUE SÃO?

Dados pessoais conforme o dicionário Dício da língua portuguesa, são aqueles dados que dizem respeito à “Informação que identifica algo, alguém ou sobre si mesmo”. Conforme esta definição é possível notar que dados pessoais são um conjunto de informações pessoais identificadoras, que vão desde endereços, número de documentos, profissão, senhas bancárias, até dados de acesso à

internet, como sites visitados, compras realizadas, uso que se faz de redes sociais, entre tantos outros.

Não obstante a definição dada acima, generalista, é importante notar que o conceito de dados pessoais pode assumir uma hermenêutica dúbia, podendo o mesmo ser retraído ou expandido, sendo que para uma futura regulamentação faz-se necessário evidenciar qual conceito está sendo utilizado, de forma a tornar clara a abrangência do título legal.

1.1 Definição e diferenças quanto aos conceitos expansionistas e reducionistas

Bruno Ricardo Bioni (2015) duas definições de dados pessoais, sendo uma delas reducionista, que diz respeito a uma realidade onde a informação deve estar ligada a um indivíduo determinado e específico, devendo ocorrer portanto um individualização aliada a uma vinculação entre o dado e a pessoa. O dado, portanto, deve constituir expressão de uma única pessoa determinada.

E a segunda adota um conceito expansionista, que diz respeito a uma realidade em que os dados pessoais não necessariamente estão ligados a um indivíduo determinado e específico, e sim ao conjunto de dados ou informações que torne possível a identificação do indivíduo, mesmo que a informação o faça de forma indireta. O dado, portanto, deve constituir meio de identificação de uma pessoa, mesmo esta não sendo determinada.

A diferenciação feita acima tem implicações na identificação do conceito utilizável em uma possível regulação.

Outro fator de suma importância é contextualizar o tipo de situação a qual se pretende regulamentar, levando em consideração, por exemplo, o tipo de dados a serem tutelados e o local onde estes se encontram. De forma que um título legal específico pode utilizar os dois conceitos para regular situações e contextos diferentes.

A tabela abaixo retirada do livro “Xeque-Mate, o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no brasil” demonstra de forma bem direta a forma como o autor Bruno Ricardo Bioni (2015, p. 15) trabalha com os conceitos expansionista e reducionista de dados pessoais:

Tabela 1 - Comparação dos conceitos de dados pessoais

EXPANSIONISTA	REDUCIONISTA
Pessoa Identificável	Pessoa Identificada
Pessoa Indeterminada	Pessoa Específica/Determinada
Vínculo mediato, indireto, impreciso ou inexato	Vínculo imediato, direto, preciso ou exato
Alargamento da qualificação do dado como pessoal	Retração da qualificação do dado como pessoal

Fonte: BIONI (2015).

Partindo das definições dadas acima é possível notar que nos dois principais projetos de lei (PL4060 e PL5276) em tramitação no Congresso Nacional referentes à proteção de dados no Brasil são utilizadas definições distintas.

No primeiro deles, o PL 4060/2012, pode-se identificar uma postura reducionista: “Art 7º: Para fins da presente lei, entende-se como: I- dado pessoal: qualquer informação que permita a identificação exata e precisa de uma pessoa determinada”.

Já no segundo, PL 5276/2016, verifica-se a adoção de uma postura expansionista:

> Art 5º Para fins desta Lei, considera-se: I- dado pessoal: dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa

O que leva à conclusão que, a depender de qual projeto for aprovado, ter-se-á uma definição de dados pessoais pouco adequada sendo adotada.

1.2 Dados pessoais e dados pessoais sensíveis

Quando se fala de dados pessoais é necessário evidenciar que estes dados são compostos por vários níveis e pessoalidade, sendo que os dados pessoais sensíveis são uma subdivisão dos dados pessoais que estão sujeitas a uma maior necessidade de proteção devido a sua natureza. Os projetos de lei existentes

(PL4060/2012 e PL 5276/2012) trazem conceitos que apresentam diferenças quanto às hipóteses, porém, possuem a mesma essência.

Os dados pessoais seriam os dados que identificam ou podem identificar a pessoa conceito esse que depende da definição a ser adotada expansionista ou reducionista, sendo que os dados pessoais sensíveis vão além dessa questão adentrando em questões bem específicas do indivíduo, desde questões psicológicas a definidoras da própria identidade.

Stefano Rodotá (2008), faz essa diferenciação ao definir que dados pessoais sensíveis seriam os dados pessoais os quais dizem respeito a um aglomerado de informações referentes a opiniões pessoais sensíveis, as quais a divulgação poderia acarretar questões discriminatórias danosas ao indivíduo que as emitiu.

Danilo Doneda (2006, P. 163), por sua vez, deixa claro que os dados pessoais sensíveis são um subgênero dos dados pessoais :

> nota-se, diante dessa breve definição, que todos os dados sensíveis são dados pessoais, mas o contrário não pode ser dito. Afirma-se, também, que a violação de dados sensíveis é muito mais prejudicial para a pessoa em causa, podendo gerar danos mais intensos à sua personalidade. Outra abordagem envolve a consideração de que o mau uso de dados sensíveis pode trazer maiores possibilidades de discriminação do indivíduo

Nesse sentido a definição apresentada por Doneda parece influenciar de forma direta nos conceitos de dados pessoais sensíveis apresentadas nas propostas de regulamentação legal de coleta de dados.

2. PROCESSOS DE COLETA E TRATAMENTO DE DADOS

Os processos de coleta de dados se diversificam de acordo com o meio utilizado para a realização do mesmo. O que no passado, por exemplo, era feito por meio de formulários impressos, hoje é realizado por meios eletrônicos. Ganhou-se no tempo gasto para esta coleta, mas também quantidade de dados que podem ser coletados e na velocidade de tratamento dos mesmos.

Quando se fala de coleta de dados atualmente podemos dar como exemplo o uso de aplicativos móveis, sendo que mesmo os mais simples aplicativos estão inseridos em um emaranhado de coleta de dados, que envolve um número indefinido de empresas (o que foi comprovado através do estudo realizado pelo ICSI Haystack Panaticon) que coletam, tratam e vendem dados pessoais.

No que diz respeito a coleta de dados, especialmente por estas vias, pode-se perceber duas grandes modalidades:

A primeira diz respeito a coleta dos dados inseridos por um indivíduo de forma proposital, em um determinado banco de dados, como por exemplo as fotos postadas no Instagram, que são enviadas à plataforma pelos usuários para serem expostas aos “colegas”, mas que constituem coleta de dados por parte da plataforma.

E na segunda modalidade tem-se a coleta de dados por terceiros (*third party tracking*), que geralmente é feita por empresas (*trackers*) que participam em fragmentos do software de desenvolvimento e interação de uma determinada plataforma, ou extensão dela, de onde serão extraídos os dados e usados para propósitos diversos daqueles para os quais foram originalmente coletados.

Esse sistema é tão complexo que a relação entre as empresas (*trakers*) e as plataformas de coleta de dados em geral são intermediados por uma terceira empresa (*broker*), empresa esta que em relação com a plataforma de origem repassa os dados a uma quantidade indeterminada de empresas *trackers*.

A coleta de dados nessa segunda modalidade é ampla, podendo todos os meios digitais (notebooks, celulares, etc...) interligados fornecerem dados às empresas de *tracking*. Com os dados em mãos as empresas podem fazer os mais diversos usos do referido dado.

O exemplo mais recorrente é quando a empresa traça um perfil do usuário com fins comerciais e, por exemplo, direciona uma determinada propaganda on-line ao mesmo. Faz isso com base no conjunto de sites/conteúdo que este usuário acessou nos últimos dias.

Quando se fala de forma técnica a coleta de dados pelos *trackers* pode se dar de diversas formas, entre elas o *download* de forma indireta de uma determinada unidade de informação implantada pelo *tracker* que serve como gatilho para transmissão de determinada informação aos servidores, que por sua vez recolhem essa informação e cruzam com um conjunto de dados que se tem a respeito do mesmo indivíduo, de forma a traçar um perfil. Ocorre que esse procedimento é realizado com uma quantidade indefinida de indivíduos gerando um banco de dados bastante amplo, mais conhecido como *Big Data*.

3. HISTÓRICO DA CRIAÇÃO DE LEGISLAÇÕES REFERENTES À PROTEÇÃO DE DADOS

Segundo Garstka (2003) na obra “Autodeterminação informacional e proteção de dados’’ a necessidade de proteção de dados nasce junto ao processo de utilização e armazenamento de dados informatizados, sendo que não se trata de uma simples proteção dos dados e sim das pessoas por trás do tratamento dos dados.

Segundo o mesmo autor (2003) o esboço de proteção de dados surge inicialmente nos Estados Unidos em meados da década de 60 através de uma dissidência entre a população e o governo, fomentada por um desejo popular de evitar uma ingerência pública na esfera privada.

De forma mais específica o governo norte americano possuía planos junto ao seu departamento de estatística para cadastrar todos os cidadãos americanos em um determinado banco de dados. Entretanto, veio a público que as forças armadas era a grande interessada na criação deste banco de dados com fins de descobrir dissidentes políticos, notadamente uma consequência do Macartismo ou “Caça às Bruxas”, política norte americana de perseguição a indivíduos indesejados pelo estado.

Ocorre que ficou comprovado à época, que as agências de segurança norte americanas já haviam recolhido e tratado dados pessoais de pessoas possivelmente suspeitas, dados estes que incluíam desde o cadastro médico até o desempenho escolar. Em contrapartida a essa coleta de dados por parte das agências no ano de 1974 foi criado o Privacy Act, que restringia a ingerência estatal na coleta de dados.

O caso americano de regulamentação da coleta e tratamento de dados fez com que os demais países industrializados colocassem a questão em suas pautas legislativas, o que pode ser evidenciado pela introdução do termo “proteção de dados” na terminologia jurídica alemã através de legislação criada no estado alemão de Hessen.

Seguindo a tendência de regulação da proteção de dados a Alemanha no ano de 1978 estabeleceu a primeira lei federal sobre proteção de dados, o que foi seguido por países como França (1978), Dinamarca (1978) e Islandia (1979). Entretanto foi só com uma convenção firmada entre os membros da Comunidade Econômica Europeia no ano de 1981 que se debateu de forma clara sobre o tratamento de dados pessoais no ambiente tecnológico.

Tardiamente a América Latina também passou a criar legislações que regulam a proteção de dados, sendo o Chile o pioneiro na criação de uma legislação nesse sentido (criou a lei nº19.628 pertinente ao tema no ano de 1999), sendo seguido pela argentina (lei 25.326/2000), sendo que muitos outros países como Uruguai, Paraguai e México, também já criaram legislações nesse sentido. Enquanto que o Brasil, como vai ser objeto de análise a seguir ainda está na fase de criação legislativa (LUNO, 1996).

4. A IMPORTÂNCIA DA PROTEÇÃO DOS DADOS PESSOAIS

Quando se fala da importância da proteção de dados é possível notar que esta se dá em amplas esferas, tanto coletiva quanto individual.

Segundo Manuel Castells (2003) os moldes da sociedade atual seguem o padrão de uma sociedade informacional, ou seja, a informação organizada constitui papel central nas dinâmicas sociais, pois é através da informação que se organizam não só os meios de produção, como também se sustenta toda a organização social. Cumpre ressaltar que o evento da sociedade informacional é decorrente de um processo de expansão tecnológica iniciada na segunda metade do século XX, e que possui tendência de se expandir cada vez mais.

Esse evento é facilmente notado, por exemplo através do cruzamento e disponibilidade dos bancos de dados pertencentes aos cadastros de restrição ao crédito, além disso é possível notar como ações antes realizadas somente de forma pessoal se tornam cada vez mais acessíveis apenas ao toque da tela de um celular, ações essas que obrigam a inserção de dados pessoais nas respectivas plataformas, o que abre precedente para aplicação das técnicas de coleta e tratamento de dados evidenciada no item anterior.

Portanto em uma sociedade tão dependente e ligada à informação, a proteção de dados constitui verdadeiro instrumento de controle do próprio poder.

Nesse sentido Stefano Rodotá analisa (2008, p. 113), no prisma evidenciado acima que: “a contrapartida necessária para se obter um bem ou um serviço não se limita mais a soma de dinheiro solicitada, mas é necessariamente acompanhada por uma cessão de informações.”

Além dessa questão, pode-se analisar a importância da proteção de dados sobre um outro prisma, o individual.

Com o advento da constituição de 1988 o ordenamento jurídico brasileiro assume as prerrogativas de um estado democrático de direito, pautado na obrigação de respeito das liberdades civis e proteção dos direitos humanos / garantias fundamentais como meio de proteção da dignidade humana.

Quando se fala dos direitos e garantias acima podemos destacar o disposto no artigo 5º, X (BRASIL, 1988) que diz: “Art. 5º , X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”.

Portanto a não proteção dos dados pessoais configura ofensa à determinação constitucional, tendo em vista que a coleta de dados pode expor o indivíduo em sua intimidade e nos mais diversos aspectos pessoais.

Nesse sentido Rodotá (2008) afirma a importância da proteção de dados através de uma breve análise social, na qual coloca que as formas de coleta e distribuição de dados utilizadas contemporaneamente levam a uma reflexão e a novos apelos a consideração da privacidade.

Tendo em vista que, restringir as questões dentro da situação tradicional dos conceitos de proteção a privacidade é considerado um ato praticamente impossível. Já que, no contexto atual não se trata da simples proteção a privacidade contra as ingerências externas, ideia individualista de ser deixado só, e sim um conjunto de ingerências na esfera individual que levam a variações na dinâmica do poder.

A influência da coleta de dados se dá no sentido em que na sociedade atual os recursos tecnológicos impõem ao cidadão a inserção no meio digital através da inserção de dados, tanto na esfera na esfera pública quanto na privada.

Esse fenômeno atrelado ao grande número de meios existentes de coleta de dados, leva a reflexão da necessidade de uma ação que se adeque a realidade atual e as constantes transformações.

Sendo que somente através dessa análise será possível criar mecanismos que contrabalanceiam a dinâmica da coleta de dados inerente a sociedade atual. Por outro lado será demonstrado a seguir a importância da criação de uma legislação que regule a coleta de dados por terceiros como meio de evitar a utilização de argumentos como o de acesso a informação para que terceiros não realizem a coleta de dados de forma indevida.

5. PRIVACIDADE X DIREITO À INFORMAÇÃO

Uma comparação importante diz respeito à dicotomia privacidade x direito de acesso à informação, sendo que para se esclarecer como o ordenamento jurídico brasileiro trata dessa questão deve-se fazer uma análise dos dispositivos presentes na carta magna.

Quando se fala do acesso à informação a constituição (BRASIL, 1988) estabelece que:

> Art. 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;
> (...)
> 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

Entretanto, a mesma carta magna estabelece (Artigo 5º, X) a inviolabilidade da vida privada, honra e imagem da pessoa, estando sujeito o descumpridor a indenização decorrente do dano moral pela transgressão.

Através da análise constitucional percebe-se a coexistência entre os direitos de acesso e de privacidade, sendo que a o direito de acesso à informação constitui regra que respeita a exceção estabelecida pelo artigo 5º, X (BRASIL, 1988).

O que pode ser diretamente ligado à dinâmica de proteção de dados, tendo em vista que o referido artigo sob a interpretação de Corrêa Bittencourt (2008, p.72) estabelece que:

> direito à honra significa a proteção das qualidades pessoais do cidadão, tanto no seu aspecto interno como em relação ao conceito de sua integridade moral na sociedade. Direito à imagem consiste em resguardar o direito à reprodução da figura física de uma pessoas por desenho, fotografia, filme, etc, bem como ao conjunto de qualidades que a pessoa transmite para a sociedade

No que diz respeito ao direito à privacidade Stefano Rodotá (2008, p. 96) vai além, afirmando que no contexto do direito à privacidade existe um núcleo duro, que diz respeito a um aglomerado de informações referentes a opiniões pessoais

sensíveis, as quais a divulgação poderia acarretar questões discriminatórias danosas ao indivíduo que as emitiu, conforme podemos extrair desse trecho constante da referida obra:

> a classificação desses dados na categoria de dados sensíveis, particularmente protegidos contra os riscos da circulação, deriva de sua potencial inclinação para serem utilizados com finalidades discriminatórias

Ou seja, fica clara a existência de uma gradação dentro do conceito de direito à privacidade, sendo que o reconhecimento dessa gradação determina a necessidade de criação de títulos legais específicos para proteger as diversas formas de expressão do referido direito, o legislador nacional caminha no sentido de reconhecer essa gradação, tendo em vista que o PL 4060/2012 e Pl 5276/2016 estabelecem respectivamente nos seus artigos 7º inciso IV e artigo 5º inciso III a existência de dados sensíveis, que são na verdade uma subdivisão dos dados pessoais que tratam especificamente do núcleo duro conceituado por Rodotá (2008).

Nesse sentido a algumas modalidades de coletas de dados por terceiros vão na contramão do disposto no texto constitucional no sentido em que expõe de forma injustificada informações de cunho pessoal que possam gerar danos ao indivíduo das mais diversas formas, o que demonstra a necessidade latente de uma regularização legislativa da questão da proteção de dados.

A necessidade de regulamentação da questão da coleta de dados é de suma importância, tendo em vista que, conforme explicitado, o direito de acesso a informação poderia em algum grau justificar o acesso e coleta de dados por terceiros a dados pessoais para utilização com fins diversos do que é considerado informacional, com intuito de formação de banco de dados comerciais , por exemplo.

Tendo em vista que, como explicitado anteriormente os dados pessoais são compostos por uma ampla gama, sendo que alguns destes dados poderiam ser coletados sob um ponto de vista que não desrespeite de forma incisiva o direito à privacidade, de uma maneira que o terceiro possa utilizar o argumento de acesso à informação (claramente de má fé) para realizar algum dos procedimentos de coletas de dados. O que pode ser facilmente corrigido a partir da criação de uma legislação que regule a coleta de dados por terceiros em todos os seus níveis.

6. PROTEÇÃO DE DADOS NO BRASIL E UNIÃO EUROPEIA

Inicialmente cumpre-se destacar que a proteção de dados no Brasil atualmente não possui uma lei específica, existindo, somente, projetos legislativos, sendo os principais o PL 5276/2016 e o PL 4060/2012, enquanto que a União Europeia está na vanguarda da proteção de dados apresentando recentemente novas diretivas sobre o tema através da regulação número 679/2016 do Parlamento Europeu.

Sendo que os projetos acima mencionados e a regulação Europeia permitem o tratamento de dados por terceiros, estabelecendo as condições e termos para que ele ocorra, sendo necessária a análise dos princípios que, segundo Danilo Doneda, devem reger e nortear essa criação legislativa.

6.1 Princípios que regem as legislações de proteção de dados

As legislações em análise apresentam em seus artigos e tópicos de forma expressa os referidos princípios, exceto o PL 4060/2012 que apresenta os princípios de forma dissolvida no decorrer do corpus legal.

6.1.1. Princípio do consentimento

Segundo este princípio a autorização para utilização/tratamento de dados por terceiros somente pode ocorrer quando houver a autorização inequívoca do titular, esse princípio é adotado na regulação europeia no tópico 32 da regulação nº679/2016 (UNIÃO EUROPEIA, 2016) da seguinte forma:

> 32 - o consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrónico, ou uma declaração oral. O consentimento pode ser dado validando uma opção ao visitar um sítio web na Internet, selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais. O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento. O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins. Se o consentimento tiver de ser dado no seguimento de um pedido apresentado por via eletrónica, esse pedido tem de ser claro e conciso e não pode perturbar desnecessariamente a utilização do serviço para o qual é fornecido

Sendo também evidenciado no artigo 7º inciso I do PL5276/2016 (BRASIL, 2016):

> Art 7º - O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I- Mediante fornecimento pelo titular de consentimento livre, informado e inequívoco;

A partir da análise dos dispositivos podemos notar que a normativa europeia é mais precisa quando menciona a necessidade de consentimento do titular dos dados, sendo que a normativa europeia exemplifica a forma como pode ser dados o consentimento apresentando a hipótese de declaração de forma escrita.

Nesse sentido, a legislação brasileira é silente estabelecendo somente que o consentimento deve ser livre, informado e inequívoco, porém, sem estabelecer a forma como será levado a cabo.

6.1.2 - Princípio da Transparência

O referido princípio diz respeito à necessidade da pessoa sujeita a coleta de dados ter conhecimento de que está sujeito a esse procedimento, bem como ter informações quanto ao uso e as pessoas que terão acesso a esse dados, sendo que este princípio é de suma importância para garantia do princípio do consentimento, já que o consentimento é dependente da informação e uso dos dados sujeitos a coleta.

Nesse sentido a Regulamentação Europeia (UNIÃO EUROPEIA, 2016) no seu tópico número 39 evidencia tal princípio da seguinte forma:

> 39 - O tratamento de dados pessoais deverá ser efetuado de forma lícita e equitativa. Deverá ser transparente para as pessoas singulares que os dados pessoais que lhes dizem respeito são recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento e a medida em que os dados pessoais são ou virão a ser tratados. O princípio da transparência exige que as informações ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples. Esse princípio diz respeito, em particular, às informações fornecidas aos titulares dos dados sobre a identidade do responsável pelo tratamento dos mesmos e os fins a que o tratamento se destina, bem como às informações que se destinam a assegurar que seja efetuado com equidade e transparência para com as pessoas singulares em causa, bem como a salvaguardar o seu direito a obter a confirmação e a comunicação dos dados pessoais que lhes dizem respeito que estão a ser tratados. As pessoas singulares a quem os dados dizem respeito deverão ser alertadas

> para os riscos, regras, garantias e direitos associados ao tratamento dos dados pessoais e para os meios de que dispõem para exercer os seus direitos relativamente a esse tratamento. Em especial, as finalidades específicas do tratamento dos dados pessoais deverão ser explícitas e legítimas e ser determinadas aquando da recolha dos dados pessoais. Os dados pessoais deverão ser adequados, pertinentes e limitados ao necessário para os efeitos para os quais são tratados. Para isso, é necessário assegurar que o prazo de conservação dos dados seja limitado ao mínimo. Os dados pessoais apenas deverão ser tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios. A fim de assegurar que os dados pessoais sejam conservados apenas durante o período considerado necessário, o responsável pelo tratamento deverá fixar os prazos para o apagamento ou a revisão periódica. Deverão ser adotadas todas as medidas razoáveis para que os dados pessoais inexatos sejam retificados ou apagados. Os dados pessoais deverão ser tratados de uma forma que garanta a devida segurança e confidencialidade, incluindo para evitar o acesso a dados pessoais e equipamento utilizado para o seu tratamento, ou a utilização dos mesmos, por pessoas não autorizadas

No que diz respeito a esse princípio o PL 5276/2016de forma menos complexa evidencia em seu artigo 8º :

> Art 8º - O titular deverá ter acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizados de forma clara, adequada e ostensiva sobre, entre outros:
> I - Finalidade específica do tratamento;
> II - Forma e duração do tratamento;
> III - Identificação do responsável;
> IV - Informações de contato do responsável;
> V - Sujeitos ou categorias de sujeitos para os quais podem ser comunicados e o âmbito de sua difusão;
> VI - Responsabilidades dos agentes que realizarão o tratamento; e
> VII - Direitos do titular, com menção explícita a:
> a - acessar dados, retifica-los ou revogar o consentimento, por procedimento gratuito e facilitado
> b- denunciar ao órgão competente o descumprimento de disposição desta lei e
> c - não fornecer o consentimento na hipótese em que o consentimento é requerido, mediante o fornecimento de informações sobre as consequências negativas

Nesse princípio notamos, novamente, que o dispositivo europeu é mais detalhista que o projeto nacional, no sentido em que apesar de o PL brasileiro apresentar o cerne da questão, a regulação europeia vai além estabelecendo uma conexão entre o princípio ora analisado e o princípio da finalidade específica, apresentando regulação técnica para realização dos princípios em conjunto.

6.1.3. Princípio da finalidade específica

Segundo esse princípio os dados pessoais coletados somente poderão ser utilizados para uma finalidade específica a qual o indivíduo tenha dado seu consentimento e que tenha sido devidamente informado (princípio da transparência), estando inclusive esse princípio inserido nos artigos e tópicos destacados acima, como elementos integrantes da formulação principiológica apresentada anteriormente.

6.2 Proteção de dados sensíveis

Os dados pessoais sensíveis são submetidos a uma proteção diferenciada em todos os meios legais em análise, tendo em vista sua natureza (conforme pode ser observado pela conceituação de dados pessoais já apresentada neste artigo).

Dessa forma o PL 2060/2012 trata dos dados pessoais sensíveis da seguinte maneira: “art 12. O início do tratamento de dados pessoais sensíveis, quando não solicitado pelo titular, somente ocorrerá mediante autorização deste, por qualquer meio que permita a manifestação de sua vontade, ou na hipótese de imposição legal.”

Já o PL 5276/2016 (BRASIL, 2016) traz o tratamento de dados pessoais sensíveis como proibida exceto pelas exceções trazidas no artigo 11, que diz:

> art.11. É vedado o tratamento de dados pessoais sensíveis, exceto:
> I- Com fornecimento de consentimento livre, inequívoco, informado, expresso e específico pelo titular
> (...)
> II- sem fornecimento de consentimento do titular nas hipóteses em que for indispensável para
> (...)

Já a regulação europeia 679/2016 (UNIÃO EUROPEIA, 2016) trata dos dados pessoais da seguinte forma:

> 51 - Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais. Deverão incluir-se neste caso os dados pessoais que revelem a origem racial ou étnica, não implicando o uso do termo «origem racial» no presente regulamento que a União aceite teorias que procuram determinar a existência de

> diferentes raças humanas. O tratamento de fotografias não deverá ser considerado sistematicamente um tratamento de categorias especiais de dados pessoais, uma vez que são apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular. Tais dados pessoais não deverão ser objeto de tratamento, salvo se essa operação for autorizada em casos específicos definidos no presente regulamento, tendo em conta que o direito dos Estados-Membros pode estabelecer disposições de proteção de dados específicas, a fim de adaptar a aplicação das regras do presente regulamento para dar cumprimento a uma obrigação legal, para o exercício de funções de interesse público ou para o exercício da autoridade pública de que está investido o responsável pelo tratamento. Para além dos requisitos específicos para este tipo de tratamento, os princípios gerais e outras disposições do presente regulamento deverão ser aplicáveis, em especial no que se refere às condições para o tratamento lícito. Deverão ser previstas de forma explícita derrogações à proibição geral de tratamento de categorias especiais de dados pessoais, por exemplo, se o titular dos dados der o seu consentimento expresso ou para ter em conta necessidades específicas, designadamente quando o tratamento for efetuado no exercício de atividades legítimas de certas associações ou fundações que tenham por finalidade permitir o exercício das liberdades fundamentais

A partir da análise dos artigos acima, resta clara a possibilidade de coleta e tratamento de dados sensíveis por terceiros, desde que esta cumpra com os requisitos apresentados nas respectivas legislações.

Nesse sentido ambas as legislações exigem o amplo consentimento do titular dos dados sensíveis como pré requisito a possibilidade de tratamento de dados pessoais sensíveis por terceiros, sendo inclusive vedado o tratamento de dados pessoais sensíveis na regulação europeia sem o fim de promover o exercício de liberdades fundamentais.

Sendo que a diretiva europeia estabelece a possibilidade de cada estado membro estabelecer critérios específicos para seu território em decorrência de peculiaridades culturais de cada estado, no que diz respeito ao tratamento de dados pessoais sensíveis por ente estatal. Enquanto que, no PL brasileiro existem algumas possibilidades de tratamento de dados pessoais sensíveis, elencadas no inciso II, que não necessariamente necessitam do consentimento do titular.

CONCLUSÃO

Podemos observar que o conceito de dados pessoais varia no que diz respeito a dinâmica adotada (expansionista e reducionista), sendo que os dois

projetos de lei analisados neste artigo apresentam definições distintas, sendo que PL 4060/2012 adota uma postura reducionista, e o PL5276/2016 uma postura expansionista. Ambos os projetos estabelecem, assim como a regulação europeia 679/2016 proteção diferenciada em relação a coleta de dados pessoais sensíveis por terceiros, devido ao fato de este tipo de dados pessoal conter informação diferenciada, .

E possível notar a partir da análise histórica, que o Brasil está atrasado no sentido de criar uma legislação pertinente a proteção de dados, estando atrás inclusive de outros países da américa latina. Tendo em vista que constitucionalmente existe um substrato para proteção a intimidade, porém não existe uma legislação específica que trate da questão da proteção de dados pessoais e pessoais sensíveis da coleta por terceiros.

Quando passamos a análise comparativa entre os projetos de lei existentes no Brasil e a legislação europeia e possível notar como a legislação europeia está consideravelmente a frente dos projetos de lei nacionais, sendo que o PL 5276/2016 se mostrou mais completo e específico que o PL 4060/2012. Com isso concluímos que é importante a aprovação de um dos projetos de lei que regem a proteção de dados pessoais da coleta por terceiros, tendo em vista não só a importância da matéria, mas também o fato de não haver no ordenamento nenhuma legislação específica que regule o tema.

É importante destacar que mesmo com a aprovação de um dos projetos de lei a matéria deve, da mesma forma que é feito na legislação europeia, estar sempre sujeita a evoluções e reanálises, tendo em vista que a matéria em questão é conexa ao meio tecnológico que se encontra em constante mudança, devendo a norma estar pronta a regular as novas evoluções técnicas.

REFERÊNCIAS

BIONI, Bruno Ricardo. **Xeque Mate:** O tripé da proteção de dados pessoais no jogo de Xadrez das iniciativas legislativas no Brasil. São Paulo:GPoPAI, 2015

BITTENCOURT, Marcos Vinícius de Corrêa. **Curso de direito constitucional**. 2.ed., ver. e ampl. Belo Horizonte: Fórum, 2008.

CASTELLS, Manuel. **Sociedade em Rede***:* A Era da Informação – Economia,Sociedade e Cultura. v. 1. Rio de Janeiro: Paz e Terra, 2003.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

GARSTKA, Hansjürgen. **Autodeterminação informacional e proteção de dados** Bonn: , 2003.

MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 4. ed. rev. e atual. São Paulo: Saraiva, 2009.

PEREZ LUÑO, Antonio-Enrique. **Ensayos de Informática Jurídica**. México: Biblioteca de Ética, Filosofia del Derecho y Política, 1996.

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

SARDENTO, Patrícia. **A proteção de dados pessoais em debate no Brasil,** disponível em: http://www.ambito-juridico.com.br/site/index.php?nlink=revistaartigosleitura&artigo, acesso em 09/11/2017

TEIXEIRA, Lucas. **Estudo de Princeton expõe vigilância descontrolada dos Trackers na Web,** disponivel em: https://antivigilancia.org/pt/2016/06/webcensus/, acesso em: 06/11/2017