MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE CIÊNCIAS JURÍDICAS
FACULDADE DE DIREITO DO RECIFE

André Luís Martins Bezerra

A lei 13.709/18 e os Novos Desafios da Proteção de Dados Pessoais e Identidade

Recife, 2019

André Luís Martins Bezerra

A lei 13.709/18 e os Novos Desafios da Proteção de Dados Pessoais e Identidade

Monografia apresentada como requisito parcial para Conclusão do Curso de Bacharelado em Direito pela UFPE.

Área de Conhecimento: Direito Civil, Direito Digital

Orientador(a): Prof. Paul Hugo Weberbauer

Recife, 2019

André Luís Martins Bezerra

A lei 13.709/18 e os Novos Desafios da Proteção de Dados Pessoais e Identidade

Monografia Final de Curso

Para Obtenção do Título de Bacharel em Direito

Universidade Federal de Pernambuco/CCJ/FDR

Data de Aprovação:

_____

Prof.

_____

Prof.

_____

Prof.

à LUIZA e ALEXANDRE, meus pais

AGRADECIMENTOS

A realização deste presente trabalho é fruto de um árduo trabalho de pesquisa, entretanto, não somente o meu labor foi o suficiente para que ele fosse completo, é essencial direcionar meus agradecimentos as pessoas e instituições que me apoiaram durante não só a produção deste projeto, como também durante minha vida acadêmica.

Por meio deste, venho agradecer ao Centro de Ciências Jurídicas da Universidade Federal de Pernambuco por promover um ambiente acadêmico fértil à pesquisa, além de me instruir magistralmente durante o decorrer do curso. Gostaria de agradecer ao professor Paul Hugo Weberbauer pela orientação desta monografia em todos os seus aspectos.

Devo também dar os devidos agradecimentos a Luiza e Alexandre, meus pais, pelo seu apoio, sacrifício, paciência e dedicação que me proporcionaram acesso a uma educação de excelência, tesouro que guardarei para o resto da vida.

Por fim, agradeço aos amigos do Movimento Lúdico que me acompanharam pelos anos de faculdade, fazendo desta uma experiência inesquecível e de engrandecimento pessoal. Amigos que levarei comigo para sempre.

RESUMO

A presente monografia de conclusão de curso surgiu como um produto da averiguação do atual contexto tecnológico que o mundo se encontra. Diante das transformações digitais, a percepção do que é ser humano vem se alterando, transformando-se de acordo com as novidades tecnológicas que influenciam e transformam a vida cotidiana, ensejando uma resposta por parte do Direito para responder as questões de como a identidade humana se comporta diante deste novo mundo e como a lei está apta a responder às novas problemáticas suscitadas, a fim de proteger os elementos formadores desta identidade como a privacidade e os dados. Diante deste questionamento esta monografia vem analisar se as bases princiológicas das novas legislações conseguirão proporcionar aos indivíduos a proteção necessária de sua privacidade e dados, bem como averiguar se ela se encontra em sintonia com os novos paradigmas propostos pela modernidade transformada pelos avanços tecnológicos, para a que proporcione uma vida plena ao indivíduo.

Palavras chave: Identidade, dados, privacidade, tecnologia.

SUMÁRIO

1. INTRODUÇÃO

A tecnologia, em seu estado atual, influencia cada vez mais a vida dos indivíduos de forma que com a criação de novos meios e reinvenção dos antigos, fez surgir uma nova problemática em relação ao modo de como são utilizadas estas tecnologias.

Um dos maiores avanços recentes na comunicação humana é a popularização da Internet e a revolução tecnológica de massas trazida por ela. O que em seus primórdios era de acesso restrito e para fins específicos, veio a se tornar um meio de comunicação massificado englobando em si inúmeros aspectos da vida cotidiana como trabalho, estudo, comunicação, lazer e comercio, de modo que é impossível para as gerações mais novas conceberem um mundo sem o uso de ferramentas de comodidade como sites de buscas, enciclopédias eletrônicas, sites de entretenimento, serviços de *streaming* e redes sociais.

Certamente, com o maior uso de atividades dependentes do meio virtual, uma serie de atividades próprias do funcionamento da rede tomaram forma. Surgidas das próprias peculiaridades técnicas da Internet, estas novas fronteiras permaneceram sem uma real atenção pelo Direito, este sempre tão tradicional e conservadora, pareceu demorar a versar sobre estas novidades trazidas pela Era da Informação em um primeiro momento, entretanto, a crescente necessidade fez com que uma maior atenção fosse dada a este novo ramo do Direito.

Com o crescente uso do meio virtual, mais e mais informações circulam na Grande Rede de Computadores, informações estas que podem ser de suma importância para o usuário, resguardada sua defesa pelo dispositivo da privacidade, que apesar de ser antigo, nunca havia sido posto a tanta prova se levar em consideração que a circulação de informação num mundo pré-Revolução Digital era mais difícil e reservada e em menor volume.

Há de se falar que existe uma certa ingenuidade dos usuários quanto a capacidade de captação e circulação de informações no meio virtual, abrindo um maior espaço para que suas informações acabem em posse de terceiros.

Atribui-se isso ao fato de que ainda se acredita em uma cessão entre o “mundo real” e o “mundo virtual” e na incomunicabilidade destes, mas é evidente que na medida que avançamos, cada vez mais dependente de tecnologia, a integração entre estes dois mundos não é só inevitável, como também ocorre em uma velocidade bem maior do que o ser humano pode compreender. Mesmo relegado ao campo da ficção, a ideia de um mundo totalmente conectado é cada vez mais palpável.

Nas vias práticas, por própria particularidade do funcionamento dos computadores, informações são arquivadas e catalogadas por tempo indeterminada, sendo possíveis que, mesmo involuntariamente, informações e dados das pessoas que utilizam as máquinas sejam sabidos por terceiros como administradores de redes e sites.

Com certo tempo de uso, baseado nas atividades que a pessoa desenvolve na rede é possível traçar perfis completos das pessoas, como seus padrões de compras, assuntos que se interessa, locais que costuma frequentar, renda aproximada, posicionamento político e diversas outras informações das mais variadas espécies.

Estes dados por si só não representam muito se desconexos, entretanto, a compilação destes pode configurar um verdadeiro atentado ao direito à privacidade individual, pois é direito do indivíduo que, mesmo que não seja de relevância, suas informações sejam vistas como sigilosas, não sendo de importância de terceiros, independentemente de qualquer propósito que se possa ter.

Este aspecto torna-se ainda mais complicado com o fato de que a informação das atividades dos usuários se tornou uma espécie de commoditie para anunciantes e políticos que, através de um perfil traçado pela coleta das informações, pode direcionar propagandas campanhas, de produtos e de serviços específicos para o usuário, independentemente do seu consentimento. Não raramente vemos anúncios e propagandas que estranhamente parecem encaixar-se perfeitamente aos nossos gostos e preferências resultantes desta troca de informações que ocorre de maneira descontrolada, regida por algoritmos..

Com esta hipervigilância o indivíduo sofre um processo de despersonalização, onde perde o direito exclusivo sobre sua personalidade, sendo ele existente além de sua esfera pessoal, com a criação de um *doppelgänger* virtual e público recriado a partir da reconstrução e cruzamento dos dados captados por terceiros.

Além da infração sobre o direito da personalidade, há ainda a preocupação sobre a capacidade de controle das escolhas visto que, com empresas que conhecem o indivíduo melhor que ele próprio, há de se falar na possibilidade que essas informações sejam usadas para um controle social direcionado.

Diante desta problemática, a analise da atual conjuntura de privacidade bem como analise da legislação se faz necessária para que possamos ter uma nova perspectiva acerca do paradigma da privacidade, bem como entender como a legislação aborda as soluções para este problema.

2. A IDENTIDADE NA ERA DA INFORMAÇÃO

A construção da identidade humana pode ser considerada uma das maiores incógnitas na qual a humanidade se deparou, seu processo evolutivo e desenvolvimento são temas de debates e especulação não só pela comunidade médica que investiga o tema de um ponto de vista científico, como também é tema de discussão para as mais diversas áreas que passam pela filosofia e sociologia com o intuito de decifrar a essência da consciência humana.

Sendo o humano dotado de sapiência sobre sua própria sapiência é natural o aflorar de tal curiosidade como tentativa da humanidade de decifrar suas próprias inseguranças ao explorar os mecanismos da própria construção identitária. A contemplação da própria identidade serve como um espelho para a personalidade humana, um ser que vê em si próprio a dúvida da existência e da consciência.

Pode-se falar que a construção de uma identidade pessoal é um conjunto de fatores, onde tanto os elementos internos e externos se equivalem no processo de evolutivo da consciência humana sobre si mesmo.

Assim como os elementos inatos e características herdadas por filiação, a inserção do indivíduo na sociedade o molda aos costumes e ideias pré-existentes do ambiente em que ele é criado, demonstrando uma dualidade na formação de cada ser humano, daí derivando a sua personalidade, ajudando-o a criar uma imagem de si próprio e do mundo que o cerca que, neste tópico, afirma Manuel Castells “A construção da identidade vale-se da matéria-prima fornecida pela história, geografia, biologia, por instituições produtivas e reprodutivas, pela memória coletiva e por fantasias pessoais, pelos aparatos de poder e revelações de cunho religioso.” (CASTELLS, 2018).

Sendo os elementos internos um tópico que está muito além do escopo deste projeto, é possível fazer algumas ponderações a cerca dos elementos exógenos, visto que, sendo todos nós humanos capazes de experimentar o mundo, todos temos a possibilidade de julgar e metrificar os elementos que percebemos em nosso exterior.

De certa forma, como fora dito, parte da identidade do indivíduo vem do meio em que se encontra e, se pararmos para fazer uma analise temporal, este ambiente historicamente sempre carregou um caráter de limitação, pois, por boa parte da história humana o indivíduo não tinha muitas oportunidades de sair do sua terra natal por razões práticas: contato com outras comunidades era algo que demandava um gasto de tempo e recursos que muitas vezes não era justificado e, em alguns casos, hostil.

Não contribuía o fato de que o indivíduo, inserido em sua própria comunidade desde seu nascimento, não via real vantagem em contato com outra comunidade visto que aquela que ele participava já lhe proporcionava tudo que ele necessitava, ironicamente, por que a própria comunidade já havia lhe incutido no subconsciente que todas as suas necessidades estariam supridas pela própria comunidade.

Com o lento avanço da comunicação entre comunidades cada vez mais a empreitada de comunicação entre sociedades torou-se uma empreitada menos custosa e, com este fato, os indivíduos estavam lentamente sendo expostos a novas culturas e ideias, rompendo com o domínio da sua comunidade de nascença sobre a segunda parte da formação de sua identidade.

Com um salto temporal para hoje, a tecnologia da comunicação chegou a tal ponto onde a conectividade proporcionada pela globalização revolucionou o modo com indivíduos interagem com comunidades que não aquelas que nasceram, o elemento exógeno que compõe a sua personalidade está cada vez mais ligada a elementos cosmopolitas e diversos, ainda mais se levarmos em consideração o quão cada vez mais jovem as pessoas são introduzidas a estas tecnologias de conexão.

Podemos citar a Internet como a maior revolução da comunicação e conectividade da história humana que, devido a sua relativa recente popularidade e disseminação, ainda há de ter seus efeitos sobre o indivíduo totalmente compreendido, entretanto, já é notável. Se antes o individuo era moldado por uma comunidade fechada em si mesmo, como será a construção de um individuo criado em uma sociedade onde as barreiras físicas tornaram-se obsoletas com a criação de um ciberespaço de um virtual trânsito livre de ideias e personalidades? Mesmo sendo ainda muito cedo para fazer qualquer tipo de afirmação concreta, é possível supor que a introdução da Internet venha a transformar não só a construção da identidade como também mude até mesmo o próprio conceito de identidade e consciência a medida que o global substitui o local e o virtual substitui o físico.

O avanço tecnológico segue a passos largos, aparelhos como telefones celulares e computadores pessoais tornaram-se cada vez mais baratos, poderosos e populares, tornando-se comuns e totalmente integrados a vida das pessoas. Seguindo nessa onda de popularização da tecnologia, a Internet se propagou a ponto de se tornar de um serviço de luxo para uma parte integral da nossas vidas tal como eletricidade e água encanada um dia foram e, se levarmos em conta que nosso aprendizado, lazer, comercio e até serviços e cadastros de órgãos públicos se fazem cada vez mais por meios digitais, não seria nenhum

disparate argumentar que o direito ao acesso a Internet se tornou essencial para o exercício da cidadania, conceito que é corroborado pela legislação brasileira na forma do *caput* do artigo 7º da Lei 12.965/2014, o Marco Civil da Internet[1]. Naturalmente, com o crescente número de internautas e com o surgimento das redes sociais, a construção das identidades veio a sentir os efeitos de um mundo cada vez mais interconectado, ganhando também uma nova dimensão de existência, a existência virtual.

Atualmente podemos afirmar que o ser humano vive em dois planos de existência simultaneamente: o físico e o virtual. O primeiro é o clássico, limitado pela presença corpórea do indivíduo e temporal, onde ele carrega consigo sua identidade da qual ele é indissociável, o segundo é meio digital que, em contraste com o físico, não se limita pela presença física de seu indivíduo, bem como possui um caráter atemporal, sua identidade pode ser acessada a qualquer momento em qualquer lugar do globo, teoricamente, qualquer pessoa.

Sendo a identidade o conjunto de percepções que o indivíduo tem sobre si mesmo, gerados a partir de suas características biológicas e sociais, podemos argumentar que as informações sobre o indivíduos – seus dados pessoais – são o componente chave para a identificação do individuo perante ele mesmo e perante a terceiros e, num mundo onde a identidade existe física e virtualmente, também é o caso dos dados pessoais.

O cerne da questão repousa no modo de como o indivíduo retém a propriedade sobre seus dados que, anteriormente se condensavam exclusivamente na figura da pessoa, uma vez que agora essas informações privadas também se encontram no *doppelgänger* virtual por meio de suas postagens em redes sociais, informações gravadas e armazenadas em bancos de dados de empresas, histórico de compras catalogados por bancos e localização monitorada por GPS embutido nos aparelhos celulares, todos esses fatores contribuindo para a criação de um dossiê digital, um simulacro da identidade real que não mais se encontra na propriedade do seu titular, ocorre uma efeito de despersonalização, onde o indivíduo perde a propriedade exclusiva sobre seus dados – por consequente a sua identidade – sendo eles utilizados por terceiros com interesses muitas vezes monetários, utilizando deste persona virtual como um alvo para o direcionamento de propagandas, serviços e, em alguns casos, influencia no comportamento pessoal como no caso de corridas eleitorais ou votações por meio de

[1] *"Art. 7º O acesso à Internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos"*

propaganda política direcionada (BUMP, 2018)[2] para convencer o alvo destas ações a tomar decisões.

Revela-se que os dados pessoais se tornaram um novo tipo de ouro digital, a possibilidade da coleta e do processamento de dados pessoais proporciona à empresas e governos a capacidade não só de entender o comportamento dos indivíduos, como também podem os influenciar tomando ações sutis para criar uma ilusão de escolha para a pessoa, uma vez que todos os seus dados tornaram-se acessíveis por meio de seu "gêmeo digital", essas entidades usam seu poder de processamento para seus próprios interesses. Esse novo mercado trilha uma linha perigosa entre o legal e a vigilância, fato que não deixou de ser notado, principalmente na atual Era da Informação

> "The increasing thirst for personnal information spawned the creation of a new industry: the database industry, na Information Age bazar where personal data collections are bartered and sold. Marketers "rente" lists of names and personnal information from database companies, which charge a few cents to a dólar for each name." (SOLOVE, 2004)

Diante deste fato, pode-se concluir que há um real perigo para a privacidade dos dados pessoais, ainda lavando-se em conta que o avanço tecnológico acelerado faz com que cada vez mais a capacidade de obtenção, armazenamento e processamento destes dados se dê de forma em que não só as pessoas não saibam lidar com este novo paradigma, como também a própria legislação, por seu processo moroso, não esteja preparada para prevenir abusos, visto que, a proteção de dados, por sua vez componente essencial para a formação da imagem e identidade do indivíduo, é algo que se deve salvaguardar para que seja proporcionada a plena experiência humana para o indivíduo.

Com a atual configuração tecnológica, a demanda pelo fluxo de informações aumentou exponencialmente não por design, mas por necessidade derivada da própria arquitetura dos sistemas e da configuração de armazenamentos na qual os bancos de dados se constituem. Desde muito tempo empresas e governos coletam dados e informações sobre as pessoas em forma de cadastros, sensos, lista de e-mail, históricos médicos, históricos de transações bancária e qualquer outro tipo de cadastro que fosse necessário para a identificação de um usuário de um serviço.

O que ocorre é que com a capacidade computacional atual, o cruzamento e o processamento de dados se tornou algo quase impossível de ser controlado, dificultando que o

[2] *"Combining the precision of data analytics with the insights of behavioral psychology and the best of individually addressable advertising technology," the company's website pledges, "you can run a truly end-to-end campaign." And that is why Cambridge Analytica was created."*

indivíduo possua alguma forma de decisão na forma que seus dados são compartilhados e usado por entidades que, muitas vezes, não pedem autorização para tal.

O que se pode afirmar a partir disto é que o indivíduo passa por um processo de despersonalização ao lhe ser retirada a propriedade e o controle exclusivo de seus dados para que seja criada uma aproximação virtual do seu real ser. Há um certo sentimento de ansiedade constante nessa despersonalização, uma suspeita constante de falta de controle da própria personalidade e de constante vigília por meio dos dados, "dataveillance": "Dataveillance is thus a new form of surveillance, a method of watching not through eyes or the câmera, but by collecting facts and data." (SOLOVE, 2004)

Mesmo em um primeiro momento, a despersonalização pode parecer apenas um efeito inofensivo justamente por se tratar de um conceito abstrato como também suas reais consequências ainda são obscuras pela falta de documentação e pro se tratar de um problema recente, entretanto, é possível ver que há um certo perigo a espreita, algo que vá vilipendiar os mais básicos dos direitos e, por isso, o Direito não pode se furtar de versar sobre.

Revela-se então que seja necessária uma analise dos atuais paradigmas da privacidade e como a legislação aborda este tema para que se possa fazer uma analise completa de se a norma jurídica está apta a media os conflitos vindouros e se o atual paradigma da privacidade tal como conhecemos ainda é suficiente para que seja usado de forma que proteja os indivíduos de abusos e permita-os viver de forma plena.

Em um cenário onde o atual panorama da identidade no mundo moderno e suas novas nuancem em relação à matéria do Direito, é importante levantar o questionamento a cerca de como a personalidade jurídica se desdobra em relação às atuais transformações tecnológicas e seus impactos no Direito.

Em seu conceito, a personalidade jurídica é algo inerente ao ser humano, sendo ele ao mesmo tempo fonte e receptáculo onde essa personalidade se manifesta, visto que, por boa parte da história, a personalidade humana e o seu agente eram indissociáveis, fato que vem se transformando a medida que as inovações tecnológicas transformam a experiência humana.

A personalidade jurídica opera de forma onde o indivíduo é tanto alvo e agente; por possuir personalidade jurídica ela é protegida pelo ordenamento, por ter personalidade jurídica ele pode exigir seus direitos, fatos que ingressam totalmente o ser humano sob a tutela do Direito.

Se hoje se vê um gradual separação entre indivíduo e personalidade, não seria de todo estranho afirmar que este fato também pode afastar o indivíduo de sua personalidade jurídica,

já que a personalidade jurídica advém da sua personalidade individual e, mesmo que versem sobre dois aspectos distintos – o indivíduo inserido no direito e o individuo com imagem de si próprio – tem uma correlação que, mesmo que simbiótica, ainda sim apartada.

> "Apesar de ambos os conceitos de personalidade (personalidade jurídica e personalidade propriamente dita, sinônimo de personalidade humana) relacionarem-se intensamente como corretamente aponta Capelo de Sousa, pois, para que o ser humano possa ser sujeito de direito, torna-se fundamental a tutela de alguns bens fundamentais da sua personalidade como identidade, a liberdade, a vida, a igualdade e tantos outros, os dois conceitos de personalidades vistos acima regulamentam bens e situações substancialmente diversas." (ROBL FILHO, 2010)

O distanciamento da personalidade acaba por infringir a própria autonomia da vontade do indivíduo, elemento fundamental para que haja o negócio jurídico, afastando de uma teoria da vontade, sendo substituído por uma teoria meramente declaratória.

> "Duas correntes se formaram, especialmente na Alemanha. Enquanto os componentes da teoria da vontade (Willenstheorie) entendem que se deve prequirir a vontade interna do agente, vontade real (Savigny, Windsheid, Dernburg, Unger, Oertmann, Ennecerus) de outro lado, os partidários da teoria da declaração (Zittelmann). Para estes, qualquer declaração obriga, ainda que por mero gracejo; para os primeiros cumpre pesquisar a realidade, seriedade etc., da verdadeira vontade." (PEREIRA, 2010)

A substituição de uma teoria da vontade por uma declaratória se encaixa facilmente em um panorama em que, por meio da utilização de nossos dados, agentes terceiros podem criar estratégias para influenciar a decisão dos indivíduos e induzi-los a tomar decisões que não necessariamente representem com fidedignidade suas reais intenções, mas um simulacro, uma representação ilusória de uma decisão tida exclusivamente pela vontade.

A tecnologia acaba por proporcionar uma quebra com a autonomia da vontade, conceito este que é algo essencialmente derivado do espírito humano e que dele deveria ser indissociável, pois é a vontade a expressão da alma humana e separa-los tira do homem não só sua autonomia, como o relega a torna-lo um ser que não mais é protagonista em sua consciência, sendo passível e de liberdade limitada por outros.

> "Por isso, a vontade humana pode ser designada como a faculdade espiritual, que o homem possui de afirmar os valores intelectualmente conhecidos ou de tender para eles. Seu objeto característico é o da vontade em geral; o ser como valor, mas apresentado segundo o modo peculiar do conhecimento e do entendimento humano.Enquanto o apetite sensitivo (tendência) se restringe ao estreito domínio de bens sensivelmente aceitáveis, a vontade tem um domínio objetivo ilimitado. Com efeito, pode dirigir-se somente àquilo que de algum modo aparece como bom, mas também a tudo quanto possua esta qualidade; ora isto é o que constitui o domínio ilimitado do ente em geral, porque todo ser é, de algum modo, valioso." (PERIN JR., 2000)

Esse afastamento entre a vontade e o indivíduo acaba por cimentar que a personalidade individual é a que dá caminho à jurídica, já que é da individual que emana aquilo que a personalidade jurídica vem em um segundo momento tutelar. Visto isso, há de se

concluir que, uma vez que os elementos que dão origem a personalidade jurídica não estejam mais em controle total do indivíduo, há um real risco a sua personalidade jurídica e a sua autonomia da vontade, fato que se levado a um extremismo lógico, representa um perigo à própria segurança de seus direitos individuais e negócios jurídicos.

Há limitações para conjecturar quais seriam os efeitos práticos de uma personalidade jurídica baseada em uma personalidade e identidade que não mais se concentram em um indivíduo e agora se manifesta por meios que estão além da propriedade do indivíduo, mas é certo afirmar que despersonalização proveniente dos meios tecnológicos pode ter consequências diretas sobre os aspectos jurídicos em alguma forma já que a base para a titularidade de direitos tem como base a personalidade do ser humano, que lhe proporciona personalidade jurídica

Com isso, uma analise da legislação à luz dos novos paradigmas da personalidade e identidade se torna cada vez mais necessária, uma vez que estes dois aspectos humanos são a base para a ciência jurídica.

3. O PARADIGMA DA PRIVACIDADE

O paradigma da privacidade remete a defesa de sua inviolabilidade, fato consagrado pela Constituição e por leis que dela derivam. Não é raro ver que há uma preocupação na defesa do foro intimo do indivíduo, visto que é daí que o ser humano constrói a si mesmo como pessoa.

Em uma perspectiva histórica, a atual conectividade excessiva da vida moderna proporcionada pela Internet e aparelhos eletrônicos pode ser visto como uma anomalia já que, por via de regra, a vida social humana se restringia a comunidades limitadas em sua maior parte rurais, sendo a urbanização um fator recente, que aglutinou a população em espaços mais próximos, onde as interações se tornaram mais frenéticas e integralizadas, fato que criou uma maior necessidade da proteção de uma intimidade que cada vez mais se esfacelava à medida que a vida urbana concentrava mais e mais pessoas. Talvez seja exatamente por se tratar de um problema nativamente moderno que vejamos uma maior preocupação com a privacidade por juristas em um mundo pós Revolução industrial, onde a onda de urbanização de fato toma propulsão.

Como marco para o avanço da discussão do direito a privacidade em um mundo de constante conectividade e avanço tecnológico podemos falar no termo cunhado pelo juiz americano Thomas Cooley; *“the right to be let alone”* (direito de ser deixado só, em tradução

livre) em 1880, termo que mais tarde foi expandido por Samuel D. Warren e Louis D. Brandeis com um artigo intitulado "*The Right to Privacy*" onde os autores colocam em evidência a ocorrência de transformações sociais, políticas e econômicas, bem como o surgimento de novos inventos, como a fotografia, que contribuíram para a ocorrência de violações da vida privada das pessoas (ZANINI, 2015).

Para os referidos autores, a criação de novos modos de difusão da informação proporcionados pelas novas tecnologias, ao invadirem a intimidade de outrem, causariam uma espécie de "sofrimento espiritual" e uma angustia que extrapolam os meros danos pessoais (FORTES, 2016).

A questão crucial deste artigo para a atual discussão a cerca da privacidade é a observação do fato que os avanços tecnológicos já eram razão para consideração jurídica já que eles poderiam vir a apresentar alguma forma de perigo à privacidade do indivíduo. Ainda mais verdade na realidade atual, onde a captação de informações e seu armazenamento se tornou o modelo padrão de negócios, retirando do indivíduo sua capacidade de reagir, pois, por muitas vezes, os agentes que retém suas informações são conglomerados econômicos ou até mesmo impossíveis de serem identificados por meio de jogadas burocráticas, desinformação e a própria ignorância sobre como seus dados são utilizados depois de serem coletados, fato que muitas vezes é promovido pelas empresas por meio de atitudes duvidosas, contratos excessivamente extensos e com pouca clareza, quando são exigidos de forma obrigatória para que seja possível a utilização do serviço prestado.

Há também de se levar em conta que o sigilo também visa proteger aspectos mais palpáveis como informações, senhas e segredos que se revelados podem causar algum dano ou por a vítima em alguma situação desfavorável, e é exatamente este o paradigma da privacidade: a proteção contra invasões para roubo de informações que possam ser usadas contra o indivíduo ou que possam gerar vantagem ilícita para um terceiro.

Em termos ilustrativos, quando se fala em invasão de privacidade sempre nos vem à mente a imagem de algum terceiro mal intencionado que, utilizando de métodos escusos como invasão, enganação, interceptação e ardil, objetiva adentrar a esfera pessoal da vítima para que possa obter informações sigilosas para fins nefastos, tal como as figuras dos estelionatários, chantagistas, *hackers* e golpistas de toda sorte.

Entretanto, com o avanço tecnológico, o paradigma da privacidade vem mudando, de forma que as figuras nefastas de outrora não são as únicas que podem se utilizar das brechas de sigilo para obter vantagem diante de alguém, a capacidade quase infinita de captação e

armazenamento de informações se tornou talvez o maior perigo a privacidade atualmente, dando-se de forma que não mais lembra o método anterior – apesar de ainda existirem e se tornarem cada vez mais sofisticados – onde um agente invadia pra obter informação, atualmente o próprio indivíduo sede seus dados de forma irresponsável, e as vezes exigida, a terceiros de forma legítima, mascaradas de cadastros, assinaturas ou até de pesquisas opinativas na qual, ao final, é necessária a inserção de dados pessoais para "validar" a resposta.

Neste aspecto, numa perspectiva contextualizada, o atual paradigma da privacidade não só deve lidar com os ilícitos de antes, como também os métodos lícitos atuais.

> "Em perspectiva histórica mais recente, Tapper (1973) identifica duas maneiras de violação de privacidade. A primeira consiste na coleta de informações pessoais a segunda concentra-se no seu uso. O primeiro modo de violação da privacidade pode ser realizado de dois modos: ilícito, quando clandestinamente, alguém coleta informações pessoais, a fim de descobrir aquelas que ainda não se tornaram públicas; lícito quando voluntariamente um indivíduo fornece informações pessoais para uma finalidade e, sem seu consentimento, tais informações são disponibilizadas para finalidade diversa." (FORTES, 2016)

Desta forma, visto que a modernidade trouxe novas formas de, até mesmo sem cometer ilicitude, burlar o direito constitucionalmente assegurado da privacidade é essencial que seja feita uma analise para que se possa averiguar se as leis vigentes no ordenamento atual são capazes de suprir a necessidade de proteção a privacidade ensejada pelos avanços tecnológicos.

Convém aqui resaltar que para uma possível analise mais precisa que produza resultados relevantes para o atual quadro em que nossa privacidade se encontra, é necessário compreender que existe certa confusão acerca do próprio conceito de privacidade visto que ela abarca duas ideias distintas que se complementam: privacidade propriamente dita e a confidencialidade.

Muitas vezes confundidas ou amalgamadas, sendo o caso da confidencialidade ainda mais gravoso já que para muitos este conceito nem se quer é conhecido, estas duas facetas conjuntamente formam aquilo que se entende a privacidade em *lato sensu*, unido duas frentes distintas sobre os dados pessoais: acesso e circulação. *"This confusion of two quite diferrent ideas. The first is controlo of access to the person. This is privacy. The second is the control of the flow of information about the person. This is confidenciality."* (FRANCIS, 2013)

Resulta desta falta de clareza da divisão e conceituação de ambos os conceitos uma confusão no momento de que vai legislar sobre qualquer aspecto que envolva privacidade. Por muito é dado importância demasiada ao aspecto de acesso a pessoa em detrimento a um maior policiamento sobre a circulação de dados, influenciando para que muitas das questões sobre a

disseminação de dados pessoais seja deixada em segunda plano quando não ignorada por completo por falta de conscientização sobre a confidencialidade.

Ainda mais gravoso se torna esta situação ao averiguarmos que o atual paradigma da privacidade se dá justamente sobre o campo da circulação desenfreada das informações, onde grandes corporações e entidades governamentais se utilizam de poderosas redes de conexão e capacidade de processamento para acelerar o fluxo de informações trocadas e compartilhadas.

> "For confidentiality, the technologies of greatest concern are capabilities for information storage and analysis. Data bases avaliable today are on an exponentially grander scale the those avaliable even few years ago, and are only growing. Data can be copied, transferred, stored, erased, or downloaded worldwide. It may be difficult or impossible to trace where data have gone and threats to data security are becoming ever-more sophisticated." (FRANCIS, 2013)

Esta falta de preocupação contra a falta de controle da circulação é justamente o que viria a causar o eventual sofrimento espiritual preconizado por Warren e Brandeis quando teorizaram seu artigo, a falta de controle sentida pelo indivíduo em relação a sua própria imagem, e é o ponto chave para a discussão de uma legislação que realmente seja eficaz na proteção destes dados.

O desafio acerca da confidencialidade se faz ainda mais evidente diante dos casos práticos. Com a popularização de aplicativos de mensagens e compartilhamento, uma modalidade de crime que fere a confidencialidade se tornou comum: *revenge porn*, pornografia de vingança, ato em que alguém, por não aceitar o fim ou interrupção de um relacionamento, divulga fotos intimas de seu alvo para que atingir sua integridade.

Pode-se dizer que não houve um ataque a privacidade da vítima já que o acesso a estas fotos foram dadas em forma de consentida, não sendo necessário por parte do criminoso ter se valido de nenhuma maneira ilegal ou ardilosa para a sua obtenção mas, se levarmos em consideração que há um acordo (mesmo que implícito por se tratar de matéria intima) de circulação exclusiva entre o casal, há um ataque a confidencialidade quando há o vazamento intencional com um intuito de ferir a dignidade da vítima. É a partir deste momento, usando esta nova modalidade de ataque a privacidade (*lato sensu*) que podemos então falar em repensar qual e como é que pretendemos defender a intimidade dos indivíduos.

Entretanto, não só os vazamentos propositais com fins pessoais podem ser enquadrados como uma ofensa a confidencialidade, há casos em que a violação a privacidade e a confidencialidade se consumam em um só ato mesmo que em momentos distintos. Um exemplo nacional é o caso da atriz Carolina Dieckman onde terceiros mal intencionados invadiram sua conta de e-mail e capturaram fotos intimas que foram usadas para extorquir a

vítima que, quando não cedeu as demandas dos criminosos, teve suas fotos vazadas (LIMA, 2016).

Dada a notoriedade deste caso, o Congresso acabou por aprovar a Lei 12.737/2012, legislação que popularmente ficou conhecida como Lei Carolina Dieckman e inseriu o artigo 154-A e 154-B ao Código Penal, tipificando o crime de invasão de dispositivos para obtenção de vantagem ilícita. Aqui, para analise, o artigo 154-A (BRASIL, Lei n. 12.737, de 30 de nov. de 2012, 2012):

> Art. 154-A. **Invadir dispositivo informático alheio**, conectado ou não à rede de computadores, **mediante violação indevida de mecanismo de segurança** e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades **para obter vantagem ilícita:**
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."

Aqui podemos ver um caso que mais se assemelha a noção habitual de um ataque a privacidade: agentes terceiros que invadam a intimidade alheia para obter vantagem e subsequentemente vemos o resultado da reação legislativa.

É possível ver que ambas as facetas são violadas no caso concreto: não só há violação a privacidade, pois o meio de acesso às informações se deu por meio criminoso por via de invasão não autorizada, há também uma subsequente violação a confidencialidade no ato de divulgação, mas, de forma não surpreendente, a legislação promulgada parece mais preocupada com apenas um dos direitos vilipendiados.

Este desequilíbrio de tratamento fica evidente no próprio *caput* do artigo ao definir unicamente sobre a invasão, listando as ações que podem ser tomadas após a invasão (como na lei: obetr, adulterar e detruir) com a finalidade de obtenção de vantagem, entretanto, não

fica evidente se isso também se aplica a questões onde a finalidade do infrator é meramente a causa de prejuízo e dano à vítima.

Há também de se apontar que o caput é bem categórico ao afirmar que é necessária a violação de algum dispositivo de segurança, podendo ocasionar na interpretação de que "acessar dispositivo alheio que não tenha, pelo menos, solicitação de senha, não constitui crime previsto no artigo, pois não haveria violação de mecanismo de segurança." (LIMA, 2016)

Em termos práticos, podemos pensar em um caso em que alguém tenha obtido as senhas e chaves de acesso por outros meios ou até negligência da vítima e usado-as para que pudesse ter acesso a informações sigilosas. Este agente ainda encorreia em crime tipificado pelo artigo 154-A? Ou ainda em algum caso como o de *revenge porn* supracitado onde as fotos íntimas estão na posse do autor desde o inicio, não precisando invadir dispositivos para vilipendiar a intimidade alheia?

Ambas as questões não podem resolvidas com base na Lei 12.737/2012, pois a lei parece não possuir uma clareza quanto a seu propósito mesmo que haja demarcado sua finalidade: a lei foi criada com o intuito de proteção a privacidade, mas efetivamente apenas trata de invasão a dispositivos eletrônicos protegidos.

Mesmo demonstrando uma preocupação em relação à proteção de dispositivos, não há como ignorar que o fato de que a privacidade e a confidencialidade ainda permanecem relegadas a uma questão acessória pela legislação brasileira até certo ponto, entretanto, a proteção destas duas trincheiras do uso das tecnologias sempre foram debatidas e analisadas.

Como foi visto, a preocupação em relação a privacidade vem desde 1890 quando foi teorizada o "direito de ser deixado de lado" e se intensificou coma chegada da Internet e dos aparelhos e aplicações que cada vez mais usavam em sua arquitetura as informações de seus usuários.

Com uma maior preocupação pela defesa da privacidade e proteção aos dados pessoais, a então na época comissária de Informação e Privacidade da província de Ontário no Canadá, Ann Cavoukian formulou e conceituou a ideia de *Privacy by Design,* um instrumento que visa guiar as pessoas com parâmetros a serem seguidos na criação de dispositivos e aplicações para que elas possam respeitar a privacidade e os dados dos usuários de forma padronizada e completa.

O conceito de *Privacy By Design* (privacidade desde a criação, tradução livre) fala sobre a necessidade de se criar sistemas que desde sua concepção integrem em sua arquitetura

mecanismos, métodos e funcionalidades que possam garantir a privacidade na *user experience* de algum aparelho ou aplicação, levando em conta a atual conjuntura de coleta e processamento de dados, de forma que a plataforma consiga garantir uma máxima experiência ao usuário e preserve seus dados pessoais.

> "Privacy, too, must be approached from the same design-thinking perspective. Privacy must be incorporated into networked data systems and technologies, by default. Privacy must become integral to organizational priorities, project objectives, design processes, and planning operations. Privacy must be embedded into every standard, protocol and process that touches our lives. This document seeks to make this possible by striving to establish a universal framework for the strongest protection of privacy available in the modern era". (CAVOUKIAN, 2010)

Para isso, Ann Cavoukian elencou em 1990 sete princípios que devem ser averiguados na criação da plataforma ou aparelho, atentando para que as opções relativas a proteção da privacidade e dos dados fossem implementadas como o padrão, totalmente integradas às funcionalidades da plataforma:

1. Proatividade, não reatividade; Prevenção, não remediação.

   Deve-se haver uma **preocupação de cuidar** para que qualquer tipo de ataque ou brecha **seja prevenido antes que aconteça**. Antecipa-se. Privacy by Design não espera infrações ocorrerem para que possa agir. Deve-se existir também mecanismos que possibilitem o reconhecimento de práticas que possam vir a ser danosa a privacidade, como método preventivo.

2. Privacidade como o *defaut.*

   Proteção de privacidade deve ser a opção padrão ao se usar uma plataforma, a proteção não precisa ser pedida pelo usuário. A informação coletada precisa ter **propósito especificado** não desviando do que foi expressamente exposto ao usuário**, coleta limitada** a necessidade da plataforma e trabalhar com o **mínimo de data** possível e ter um mínimo de uso e armazenamento para seus propósitos.

3. Privacidade incorporada ao design.

   A proteção à privacidade deve se dar de **forma harmoniosa** com o restante da aplicação, de modo que **não interfira negativamente na experiência do usuário** ou que diminua a funcionalidade. Holística, interativa e criativa, proporcionando ao usuário uma experiência completa.

4. Funcionalidade Total – soma possitiva, não soma-zero.

A proteção deve ser dada de maneira que **não haja *trade-offs*** como, por exemplo, menos proteção por mais segurança ou que o usuário **perca funcionalidade em troca de uma maior proteção.**

5. Segurança de ponta-à-ponta – proteção por todo o ciclo da informação.

   As informações devem ser asseguradas **durante todo seu "ciclo de vida"** que se inicia com o primeiro acesso a plataforma e até sua eventual exclusão, sendo a **proteção resguardada por todas as fases**.

6. Visibilidade e transparência.

   O tratamento dos dados deve ser dado com **total transparência para o usuário**, no modo como ela é coletada, processada, armazenada e **clareza no propósito e finalidade** que ela será usada.

7. Respeito à privacidade do usuário.

   O **respeito à privacidade** do usuário deve ser o **maior bem protegido** pelos operadores, sendo requerido o seu consentimento, que suas **informações sejam sempre precisas**, tendo eles **total acesso** e que seja **passível de correção ou reclamação** a qualquer momento por parte do titular dos dados.

Desta forma o Privacy by Design como idealizado por Ann Cavoukian conseguiria cobrir qualquer tipo de lacuna que poderia representar um risco ou brecha para a privacidade do usuário, garantindo-lhe total controle, transparência e segurança sobre seus dados, preservando não só o acesso a estas informações, como também a circulação desta.

Fica evidente que há uma preocupação sobre a condição que se encontra a preservação dos dados pessoais não só por uma comunidade internacional como também é algo que já se é discutido de forma madura a bastante tempo.

O caráter internacional desta discussão não é nenhuma surpresa. Além de ser algo que está presente em todos os ordenamentos do mundo, as questões de privacidade e circulação de dados também se encontram na plataforma internacional devido ao caráter globalizado das tecnologias atuais e da conectividade, que cada vez mais borra os limites nacionais.

No cenário nacional, anteriormente a lei 12.737/2012 podemos citar a lei 12.527/2011, popularmente conhecida como Lei do Acesso à Informação, como uma legislação que se preocupou em tratar da privacidade já que ela "determina que o tratamento das informações pessoais detidas por entidades e instituições nela abrangidas seja realizado de modo transparente, respeitando o direito fundamental à proteção da intimidade, da vida privada, da

honra e da imagem"[3] (FORTES, 2016), versando sobre a relação de informações do indivíduo com os órgãos do Estado, alinhada com o disposto da Constituição Federal/88 em seu artigo 5º, inciso XXXIII, artigo 37, parágrafo 3º, inciso II e o artigo 216, parágrafo 2º.

Foi então com o advento da lei 12.965/2014, o Marco Civil da Internet, é que o Brasil começou a ter uma discussão madura em relação a proteção de dados que levasse em conta o atual paradigma da privacidade na era digital.

A discussão sobre uma legislação de uma regulamentação sobre a Internet vem desde a popularização da Internet como um serviço amplamente difundido nas residências da população, sendo ensejado em 2007 pelo professor Ronaldo Lemos em um artigo quando analisava uma proposta de lei que versava sobre crimes virtuais, na época Lemos destacou a importância de se criar uma lei de regulamentação civil antes de uma regulamentação penal:

> "E uma vez mais, todo o esforço de debate público em torno de um tal projeto de lei, que tem por objetivo regulamentar a Internet do ponto de vista criminal, deveria se voltar à regulamentação civil da rede, definindo claramente o seu marco regulatório e privilegiando a inovação, tal qual foi nos países desenvolvidos. Privilegiar a regulamentação criminal da Internet antes de sua regulamentação civil tem como conseqüência o aumento de custos públicos e privados, o desincentivo à inovação e sobretudo, a ineficácia. Nesse sentido, é preciso primeiro que se aprenda com a regulamentação civil, para a partir de então propor medidas criminais que possam alcançar sua efetividade, sem onerar a sociedade como um todo, como faz o atual projeto de lei do senador Eduardo Azeredo." (LEMOS, 2007)

Mesmo com a discussão iniciada, foi apenas em 2009 que de fato começou a discussão em âmbito das instituições proposto pelo Ministério da Justiça[4], sendo então em 2011, pela então presidente Dilma Rousseff (PT-SP), formalmente apresentada uma proposta de lei que versava sobre os aspectos civis da Internet[5] (JINKINGS, 2011). Para o então ministro da Justiça, Luiz Paulo Barreto, o Marco Civil da Internet seria como uma Constituição da Internet. (Agência Estado, 2010)[6].

Mais do que meramente um regulamentação das práticas e dos atos exercidos na Internet, o Marco Civil regula os direitos e garantias dos internautas, dando especial

---

[3] *Art. 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*.

[4] "*A proposta começou a ser discutida em 2009 e foi elaborada pelo Ministério da Justiça com o apoio da Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas. O texto do projeto busca estabelecer uma regulamentação geral sobre o uso da* internet."

[5] *"A proposta, apresentada hoje (24) ao Congresso Nacional pela presidenta Dilma Rousseff, define regras para garantir os direitos dos usuários, as responsabilidades dos provedores de serviços e a atuação do Estado no desenvolvimento e uso da rede. O objetivo, segundo o Ministério da Justiça, é oferecer segurança jurídica para as relações na* internet"

[6] *"Poderemos contar, no Brasil, com uma Constituição da Internet, como uma Constituição de 88, uma Constituição cidadã", afirmou. "Podemos colocar o Brasil numa vanguarda com o marco civil da internet", acrescentou*

importância aquilo que foi tido como o essencial para a Internet, comunicação e a circulação de dados.

A regulamentação de Internet se faz necessária no momento em que se entende que comunicação e circulação de informações constituem em si uma forma de poder sobre aquele de quem as informações descrevem, logo, o agente que controla esse fluxo de informações tem uma relação de desequilíbrio em relação àquele que cede suas informações "torna-se evidente, portanto, que o poder da informação em um contexto em que a tecnologia está baseada na comunicação e na transferência de informação e dados pode ser tão nefasto quanto o poderio bélico almejado, por séculos, pelas nações, como um indicador de poder e de domínio sobre os povos" (FORTES, 2016).

O Marco Civil além de expandir exponencialmente os tópicos abarcados pela legislação brasileira em relação aos serviços prestados por provedores de Internet e sites em geral, foi instrumental na expansão da proteção de dados mais alinhado ao paradigma da privacidade, dedicando uma seção própria para a matéria, cobrindo até aquele ponto a necessidade de resguardar a privacidade do usuário diante dos possíveis abusos que pudesse surgir contra o internauta.

É possível ver que a legislação brasileira abraçou conceitos apresentados pelo Privacy by Design em sua normativa quando fala sobre dados pessoais em seu artigo 7º quando trata dos direitos e garantias do usuário (BRASIL, Lei n. 12.965 de 23 de abr. de 2014, 2014). Analisando seu caput e alguns de seus incisos podemos averiguar este fato

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

Temos aqui, de forma bem direta que o acesso a Internet foi elevado ao status de um direito fundamental ao exercício da cidadania. Deveras, com o atual quadro, boa parte de muito acessos a bens e serviços promovidos pelo governo são acessíveis somente por alguma plataforma digital, fazendo com que se torne indispensável o acesso a Internet para o exercício de uma cidadania plena.

Logo em seguida vemos em seus três primeiros incisos a preocupação sobre o sigilo da comunicação. Mesmo se aproximando mais da noção constitucional da inviolabilidade das

comunicações, no espaço virtual a comunicação também é parte integrante dos dados do indivíduo, sendo sua proteção requerida para o bom uso da Internet.

> VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
> a) justifiquem sua coleta;
> b) não sejam vedadas pela legislação; e
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
> IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
> X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;
> XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;

Do inciso VI ao XI é possível já perceber um maior foco na proteção dos dados de forma mais nominal. Interessante é resaltar que a lei é pertinente em discorrer tanto sobre o acesso quanto sobre a circulação dos dados, de forma que podemos desenhar a influência do Privacy by Design.

O inciso VI exige o respeito ao quesito da Visibilidade e Transparência no tratamento de dados, o inciso VII veta a circulação desenfreada das informações, pondo o dado como maior bem protegido, obedecendo ao quesito do Respeito à Privacidade do Usuário, o inciso VIII limita a coleta de dados, exigindo que ela seja clara e restringida a somente ao necessário conforme o quesito da Privacidade como *Defaut,* os incisos IX e X submetidos ao quesito da Segurança de Ponta-a-ponta, garantindo o cuidado com a informação desde sua coleta até sua exclusão e por fim o inciso XI mais uma vez reforçando a transparência que deve haver na relação provedor e usuário naquilo que diz respeitos ao acesso, processamento, armazenamento, circulação e exclusão de dados.

Em matéria mais específica, o Marco Civil reserva uma seção para o armazenamento dos dados pessoais, impondo limites para que seja salvaguardada a exclusividade dos dados pessoais por parte do indivíduo.

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do

> conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
> § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no **caput**, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.
> § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.
> § 3º O disposto no **caput** não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.
> § 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.

Neste artigo é possível averiguar que a norma se dedica a proteção dos dados mas o faz de forma que também leva em conta as questões judiciais, impondo um limite ao sigilo quando este precisa ser relativizado. Entretanto isso ocorre expressamente mediante a decisão judicial e, de nenhuma forma fere a proteção concedida pelo ordenamento, visto que a liberação das informações sensíveis é tratada como exceção, sendo necessário aporte legal para que possa ser relativizada. Isso demonstra que a legislação respeita a privacidade na medida que ela é usada para proteger o direito do indivíduo, não de ações que possam vir a serem danosas, perpetuadas no ambiente virtual.

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
> § 1º O disposto no **caput** aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
> § 2º O disposto no **caput** aplica-se 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.
> § 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.
> § 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

O ordenamento neste artigo reconhece o caráter internacional da Internet. Visto que o fenômeno da Internet ocorre em um ambiente virtual onde as divisões estatais não são exatamente claras, a legislação brasileira reconhece que mesmo que as atividades virtuais ocorram em um plano diferente daquele dos negócios jurídicos tradicionais, ainda assim há a

necessidade de regulamentação quando se trata de qualquer tipo de informação que possa ter passado por agentes que atuem nacionalmente, sendo eles suscetíveis a legislação nacional.

> Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;
> III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou
> IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.
> Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o **caput** sua filial, sucursal, escritório ou estabelecimento situado no País.

Por fim, o Marco Civil prevê punições para aqueles que desrespeitarem a privacidade e a confidencialidade consagradas pela legislação, reconhecido a importância de um ambiente seguro para a utilização das inovações tecnológicas proporcionadas pela Internet e as demais aplicações que dela derivam.

Fica evidente que a conceituação daquilo que entendemos como privacidade mudou, transformado pelas mudanças trazidas pelo avanço tecnológico e o desenvolvimento de uma sociedade virtual que se baseia na circulação implacável de informação e dados.

A discussão sobre a privacidade vem tomando novos rumos e andou um longo caminho desde as ideias de Warren e Brandeis e seu receio quando ao “mal estar espiritual” que as novas tecnologias proporcionavam ao indivíduo, mas é sempre vista como um conceito basilar para o exercício da cidadania e de uma experiência humana plena e produtiva.

O novo paradigma da privacidade nos é revelado como o novo norte que deve guiar a sua proteção. Devemos ver a privacidade não somente como um monólito, a proteção da privacidade no mundo moderno deve ser completa, desde a concepção levando-se em consideração a captação, processamento, armazenamento, circulação e uso para que possamos analisar e criar normas que estejam aptas a proporcionar uma proteção de ponta-a-ponta, garantindo o direito do indivíduo em todos os seus aspectos.

4. OS PRINCÍPIOS DA LEI 13.709/2018 E O NOVO PARADIGMA DA PRIVACIDADE

Explanado o que se pode entender sobre o novo paradigma da privacidade é de suma importância que este conceito esteja presente em uma legislação que se proponha a defesa de

um direito tão fundamental quanto importante quanto a privacidade para a atual conjuntura da sociedade.

A conectividade que testemunhamos nascer na virada dos anos 2000 tem escalas sem precedentes e impacta a sociedade de uma forma tão profunda que qualquer ideia de que se possa retornar a um mundo anterior se mostram nada mais do que meramente ilusórias. O mundo se tornou a hiperconectividade propagada por eletrônicos e cimentada pela Internet.

Neste contexto, o Direito não pôde se furtar de contemplar tais questões, justamente pelo fato de que, se tratando a ciência jurídica do estudo das leis que regulam a experiência humana, revela-se como uma questão que interfere tão profundamente nas relações humanas que há a necessidade de regulamentação para que os direitos fundamentais sejam respeitados.

Se tratando de um fenômeno global, não é surpresa ver que a iniciativa para a proteção de dados também seja em escala mundial. Mesmo sendo a legislação brasileira considerada pioneira com a promulgação da Lei 12.965/2014, o Marco Civil da Internet[7] (CALIXTO, 2014), pôde se ver um relativo silêncio das autoridades após um primeiro momento, onde se acreditava que a o Marco Civil conseguiria suprir qualquer problemática que poderia ser causada no âmbito virtual, inclusive em relação aos dados pessoais.

Ainda assim, mesmo sem uma legislação específica, era visto um esforço por parte do judiciário em manter a preservação dos dados e de sua circulação. O Superior Tribunal de Justiça, em julgamento sobre a possibilidade de compartilhamento de dados de seus clientes usuários de cartões de crédito vetou tal conduta[8] (BULLA, 2017).

Em seu voto, o Min. Luis Felipe Salomão da 4ª Turma do STJ destaca como a exposição de dados tal como o padrão de consumo dos clientes é algo importante e passível de previa autorização, sendo impedido o consentimento obrigatório por clausula contratual, algo que o ministro julgou como abusiva.

> "De fato, a partir da exposição de dados de sua vida financeira abre-se leque gigantesco para intromissões diversas na vida do consumidor. Conhecem-se seus hábitos, monitoram-se sua maneira de viver e a forma com que seu dinheiro é gasto. Por isso a imprescindibilidade da autorização real e espontânea quanto à exposição. Não bastasse o panorama traçado acima, considera-se abusiva a cláusula em destaque também porque a obrigação que ela anuncia se mostra prescindível à execução do serviço contratado, qual seja obtenção de crédito por meio de cartão." (STJ, 2017)

[7] *Os portais Global Voices e Bloomberg classificam a "A Nova Constituição para Internet" como um marco e exaltam o trabalho pioneiro. "A lei faz do Brasil o líder entre os maiores países do mundo em defesa do princípio de neutralidade de rede", afirma o Bloomberg. "A lei de direitos na Internet se tornou trending topic no Twitter após Congresso brasileiro aprovar lei pioneira para o direito dos usuários de internet".*

[8] *Em julgamento nesta semana, a 4.ª Turma do Superior Tribunal de Justiça (STJ) formou um precedente que passa a valer para contratos de cartão de crédito. O HSBC está obrigado a retirar de seus contratos padrões a cláusula que permite o compartilhamento de dados do consumidor – como hábitos de consumo.*

A preocupação acerca do sigilo dos dados pessoais também se torna algo de suma importância para a preservação da integridade individual. Em um processo de dano moral por divulgação de informações pessoais de cunho trabalhista o relator Min. Sebastião Geraldo de Oliveira julgou o Recurso Ordinário impetrado pelo Réu como improcedente, corroborando em seu voto que "a exposição de dados pessoais da autora gera constrangimentos decorrentes da imediata afetação da intimidade e vida privada da reclamante, valores resguardados constitucionalmente" (TRT-3, 2018).

Pode-se ver que até mesmo antes da promulgação da Lei 13.709/18 a discussão sobre a importância dos dados bem como sua proteção em um mundo onde a informação obteve valor em si próprio sempre ocorreu de certa forma, numa multiplicidade de campos. Também é imperioso notar que a disposição dos julgadores se dá de forma favorável a proteção que, mesmo não sendo dada por legislação específica, era respeitada como princípio constitucional.

Com o desenvolvimento de ferramentas mais sofisticadas de coleta e processamento de dados, além do acontecimento de novos casos de brecha de segurança e a circulação indiscriminada de dados por agentes com interesses ulteriores, acabaram por causar certos incidentes internacionais que expuseram a necessidade de criação de mecanismos jurídicos que pudessem assegurar com maior afinco os dados e a privacidade dos cidadãos.

Talvez como emblemático destes casos seja a brecha que ocorreu com o Facebook que deu caminho a um escândalo acerca da política de privacidade em sites da Internet e como a legislação dos países estavam aptas a suprir possíveis usos indevidos de dados pessoais.

Servindo como fato que deu início a uma discussão mais séria sobre os limites do uso de dados, este incidente foi decisivo para que a União Europeia pudesse discutir e então aprovar a General Data Protection Regulation (GDPR), um documento que pretende proteger os dados pessoais de maneira que consiga abarcar todas as necessidade atuais acerca de dados sensíveis.

A GDPR vem como sucessora da diretiva 95/46/EC, servindo como uma lei com poder coercitivo e um escopo muito mais abrangente que incorpora em seu texto noções modernas sobre captação e circulação de dados para cidadãos europeus que usem a Internet. Ainda se preocupando com a questão internacional da problemática, a GDPR foi, segundo Ronaldo Lemos, uma legislação que tem um caráter "viral"[9] (PACETE, 2018) na medida em

[9] *A GDPR pretende proteger residentes da comunidade europeia de casos como o da Cambridge Analytica que veio à tona em março e envolveu a exposição de 87 milhões de usuários do Facebook. "A regulação foi desenhada para ter efeito 'viral'. Uma vez que uma empresa passa a cumprir seus requisitos começa a exigir*

que ela pretende criar um efeito dominó, reforçando que sites e empresas, mesmo que não estejam locados dentro do território europeu, a obedeçam quando forem usadas por cidadãos europeus.

Desta forma, com sua implementação no ano de 2018, a GDPR afetou em larga escala a Internet criando um efeito cascata, demandando que os sites e prestadores de serviço se adequassem a norma.

Para o contexto nacional, a GDPR impulsionou a criação de uma legislação nacional que tratasse de proteção dos dados pessoais com uma maior abrangência do que aquela apresentada pelo Marco Civil da Internet, aprofundando a questão e criando parâmetros mais alinhados com os padrões internacionais, além do fato de que a GDPR expressamente veta empresas europeias que tratam de dados de alguma forma de fazer negócios com empresas de países que não possuíssem uma legislação específica para o tratamento de dados.

É nesta conjuntura que a legislação brasileira se viu compelida a produzir um diploma que tratasse do assunto, no que resultou com o estabelecimento da lei 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD).

Em uma analise do pré-projeto que viria ser a LGPD, Vinícius Borges Fortes faz uma comparação com as legislações europeia, analisando como a lei brasileira propunha uma maior abrangência no tratamento da matéria pela legislação brasileira.

> "Por analise comparativa das diretivas europeias, verifica-se que o rol de definições do anteprojeto de lei dos dados pessoais é significativo e consistente para abranger diversas hipóteses fáticas, relacionadas ao que o anteprojeto define como tratamento de dados. Observa-se também que o anteprojeto brasileiro recepciona o conceito do consentimento como um dos elementos de tutelados dados pessoais." (FORTES, 2016)

A LGPD busca por meio de uma série de artifícios jurídicos regular a questão dos dados pessoais e como eles são administrados, de forma que o seu intuito seja sempre o respeito aos direitos do indivíduos, tratando os dados com transparência e responsabilidade.

> "O objetivo da LGPD é o de "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade natural". O verbo "proteger" diz muito sobre a forma como o legislador enxergou o titular dos dados, ou seja, em posição desigual em relação aos resposáveis pelo tratamento de dados, ficando patente sua vulnerabilidade." (COTS & OLIVEIRA, 2018)

Este parâmetro da hiposufuciencia daquele que cede seus dados muito se assemelha ao pressuposto que norteia o Código de Defesa do Consumidor. A LGPD reconhece as limitações técnicas quase infindáveis que indivíduo tem ao tratar com um sistema tão

que outras da cadeia cumpram também", diz Ronaldo Lemos, advogado e professor visitante da Columbia University.

complexo quanto à captação e processamento de dados, muitas vezes representando um obstáculo quase instransponível entre o indivíduo e seus dados.

Esta preocupação demonstra que a LGPD está disposta a tratar a proteção de dados em um contexto atual, reconhecendo as minúcias práticas de como o usuário de tecnologia interage com as inovações tecnológicas e como se tornou integral para a atual economia baseada em informação o tratamento de dados.

Fazendo-se uma analise mais aprofundada, é imperativo que se averigue a capacidade da LGPD em respeitar a privacidade dos dados de acordo com o novo paradigma da privacidade, criando defesas e mecanismos que tratem os dados em um contexto moderno, sob o risco de uma lei ineficaz que não produzirá os efeitos desejados, pondo em risco os direitos fundamentais daqueles que visa proteger.

Logo em seu 1º artigo, a Lei 13.709/2018 delimita seu intuito e sua finalidade, abarcando os dados de pessoas naturais e jurídicas independente de sua natureza. Mesmo acreditando que a extensão desta lei para pessoas jurídicas seja algo que vai além do que seja necessário, é importante notar que o intuito da proteção dada é o resguardo dos direitos fundamentais e privacidade para o "livre desenvolvimento da personalidade da pessoa natural".

Revela-se ai a importância e a conscientização da legislação sobre como a personalidade humana se constrói em seu intimo, sendo os dados pessoais necessitados de uma especial proteção para a formação saudável do indivíduo na construção natural da sua personalidade, elemento fundamental para à experiência humana. Fica evidente que o diploma entende que o ser humano e seus dados são indissociáveis e a proteção deles é imperativa.

> "Ao proteger os seres humanos e um dos seus direitos fundamentais, que é a privacidade, está-se protegendo um ser único e complexo, totalmente suscetível às condições do ambiente, e que depende de condições adequadas para que seu desenvolvimento se dê de maneira completa e mais ampla possível" (COTS & OLIVEIRA, 2018)

O próximo artigo, artigo 2º, alinha a LGPD aos direitos fundamentais constitucionalmente reconhecidos como privacidade, liberdade de expressão, inviolabilidade da intimidade, direitos humanos e a livre iniciativa. Este ultimo é interessante pois de certa forma reconhece que há a existência de uma nova economia que revolve em tono dos dados. Neste reconhecimento a legislação não veta qualquer tipo de negócio que sua base seja dados, ela meramente prega que o tratamento deva se dar com respeito aos direitos individuais.

Os artigos 3º e 4º descrevem a abrangência e a limitação da aplicabilidade da proteção de dados. Em alinhamento com a legislação da GDPR o artigo 3º estende sua jurisdição a

qualquer operação que tenha ocorrido em território nacional, independente do meio e do país onde os dados estejam localizados. O próximo artigo limita a aplicação da lei para aplicações pessoais, questões jornalísticas e artísticas, bem como fins de segurança.

O artigo 5º se revela como algo de suma importância pois dá as definições legais dos conceitos que serão usados para definir a ação desta lei, bem como a terminologia para ações que podem ser tomadas pelos indivíduos no tratamento de seus dados.

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> 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;
> 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;
> IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
> 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;
> 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;
> IX - agentes de tratamento: o controlador e o operador;

É importante resaltar que a definição que se dá para dado pessoal é mais do que meramente considerado informação, mas adota-se uma interprestação expansiva de que dado pessoal é qualquer informação que possa distinguir o indivíduo de um grupo tornado a pessoa identificável. O que causa estranheza é o fato da lei distinguir dados pessoais em sua forma genérica e a sua forma “sensível”, mas é possível entender esta divisão ao levarmos em conta que há dados indissociáveis dos indivíduos e que surgem da própria personalidade do indivíduo.

A título de exemplo podemos entender que o padrão de compra de uma pessoa seria um dado pessoal, mas ele não coresponde a algo direto da personalidade da pessoa pois é um dado criado a partir de questões que não dependem totalmente da personalidade do indivíduo, enquanto algo sensível como ideal político deriva diretamente da alma do indivíduo e de suas experiências e reflexões, parte da sua personalidade.

O dado anonimizado se refere aos dados que passaram deliberadamente por um processo que pudesse deixar seu titular anônimo, indicando que há um interesse real em dar

um tratamento diferencial, seja lá o motivo para isso, entende-se que a lei permite esta ação a critério do titular do dado.

A lei então descreve o local de armazenamento dos dados, identificado como banco de dados, a estrutura que armazena os dados. O fato de haver uma definição da estrutura implica que há também quem o controle, agente que tem responsabilidade sobre a estrutura visto que nenhuma estrutura existe sem algum agente por trás dela.

Os incisos V a IX enumeram os agentes, passivos e ativos nas relações de transição de dados, dando especial importância para a figura do titular, figura que é o alvo da proteção desta lei e a quem é reconhecida a hipossuficiencia diante controlador, operador e demais agentes.

> 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;
> XI - anonimização: utilização de 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;
> XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
> XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
> XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
> XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
> XVI - 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;
> XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
> XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei.

Por fim do artigo 5º é listado as ações que podem ser tomadas por titulares ou demais agentes quando se tratando de dados, hipóteses que a lei prevê e que delas regulamenta. Nota-se que em seu ultimo inciso há indicação de uma autoridade nacional que seria responsável sobre as questões que envolvam dados.

Indubitavelmente, podemos ver que o artigo 6º é o que mais revela sobre como a LGPD está adaptada à proteção dos dados pessoais em um panorama onde o paradigma da

privacidade se transformou. Há enumeração de princípios que devem ser respeitados quando se trata de um assunto tão sensível a população quando os dados pessoais.

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

É aferível como este artigo usa de forma quase que completa as ideias de Privacy by Design proposta por Ann Cavoukian, sendo seus incisos carregados de similaridades com os sete princípios enumerados por ela.

É evidente que durante a formulação da LGPD houve cuidado para que a lei estivesse de acordo com um tipo diferente de noção de privacidade. A adoção de conceitos como o Privacy by Design demonstra a preocupação do legislador não só de criar mecanismos que pudessem proteger o indivíduo como também proteger o próprio dado em si, desde sua captação até sua eventual exclusão, demonstrando que é reconhecido um valor no dado em si, valor resultante da maneira de como uma sociedade altamente tecnológica e conectada percebe as informações e como elas são preciosas e dignas de proteção.

O princípio da finalidade restringe a captação do dado e para a finalidade que ele terá, demonstra-se assim uma preocupação de que mesmo que o dado seja cedido, o titular ainda mantenha controle sobre ele, evitando que haja alguma forma de despersonalização pois seu dado ainda estará sobre seu controle, sendo necessário seu consentimento para com o processo completo para ser utilizado.

O segundo inciso exige que haja compatibilidade do real uso do dado com a finalidade descrita que levou a permissão da captação do dado em primeiro lugar. Este princípio impede que o titular seja ludibriado a consentir com uso de suas informações para fins além daquele que ele concordou.

O princípio da necessidade delimita a captação exclusivamente ao necessário para as operações acordadas, vedando que sejam obtidas informações para além da finalidade, sendo um princípio direcionado a limitação daquele que captará os dados.

O quarto princípio garante o livre acesso do titular a seus dados, mais uma vez reforçando a propriedade do titular sobre seus próprios dados e total controle sobre eles. Mais uma vez há preocupação por parte do legislador em manter a conexão dos dados ao titular visto a importância destes para a formação do indivíduo e seu caráter indissociável.

O quinto inciso fala do princípio de que os dados devem ser mantidos de forma intacta, garantido sua "qualidade", a não interferência de terceiros sobre os dados do agente, sendo exigido que os dados sejam preservados da maneira que foram aferidos, produzidos ou cedidos, reforçando a titularidade do indivíduo.

O princípio do inciso sexto prevê que haja transparência durante todo o processo que os dados passam, que o titular saiba todas as movimentações de seus dados, sendo a ele garantida clareza e precisão.

O princípio da segurança exige por parte do operador medidas que reforem a segurança e a integridade dos dados e processos de captação pelo os quais o dado passará, garantindo ferramentas que possam proporcionar um ambiente seguro para o tratamento de informações.

A prevenção serve como um princípio pode ser vista como complemento a anterior, trabalhando como complemento. Assim como nos princípios da Privacy by Design, a legislação se preocupa em prevenir mesmo que preveja medidas de reação, pois entende a gravidade e do valor da informação em na sociedade moderna.

O nono inciso inova e vai além, circunscrevendo que não pode haver discriminação no tratamento do indivíduo devido a suas informações pessoais. O operador, ao ter acesso a informações do titular obtém acesso a informações pessoais e diante delas não pode dar tratamento diferenciado ao indivíduo que possa vir a prejudica-lo, garantindo ao tratamento igualitário a todos, para que eles possam circular seus dados sem receio.

De certa forma, este inciso se assemelha a Genetic Information Nondiscrimination Act americana, lei que previne que um indivíduo tenha um tratamento diferenciado por causa de

sua genética por parte de agencias de seguro ou planos de saúde[10] (Genetics Home Reference, 2019) e, levando em consideração de que informações genéticas são considerados dados sensíveis, a lei brasileira veta que os dados pessoais sejam usados contra o indivíduos visto que deles são indissociáveis.

Por fim, o artigo deixa a cargo do operador a responsabilidade sobre os cuidados das operações, bem como atender todos os princípios anteriormente citados como forma de garantir ao titular o respeito a seu direito de posse sobre os dados.

O artigo 6º é emblemático para a LGPD pois apresenta quais os princípios que regem o diploma e harmoniza a legislação brasileira com a internacional, respeitando o caráter supranacional proporcionado pela conectividade atual.

É interessante ressaltar que a legislação dá um valor especial aos dados, reconhecendo-os como um dos fatores integrais para a formação da personalidade humana e visa criar um ambiente saudável para que o desenvolvimento humano possa ocorrer de forma que lhe proporcione completude. Tão importante para a formação humana, os dados devem sempre de posse exclusiva daqueles que por direito pertencem, sabendo que expropria-lo de tais dados é um atentado a sua personalidade e a seus direitos fundamentais.

Os princípios também contemplam a questão do acesso aos dados, promovendo uma proteção a privacidade tal como resguardam ressalvas sobre o modo como essa informação circula, respeitando a confidencialidade dos dados na limitação de sua circulação dependente do consentimento do titular.

Imaginar um mundo onde o acesso e a circulação são restritos por lei em favor da preservação da identidade individual não é mais uma opção viável, as transformações tecnológicas criaram um mundo baseado na intensa circulação da informação, ensejando uma mudança no paradigma da privacidade que vemos hoje: a privacidade não apenas termina no próprio individuo, a informação em si se tornou passível de contemplação jurídica e protegê-la deve ser um dos objetivos contemplados por qualquer legislação que se preocupe em enfrentar os desafios modernos.

Desta forma, é possível averiguar que a lei 13.709/18 apresenta em seu aporte de princípios aqueles necessários para lidar com o desafio da modernidade, tratando a proteção dos dados com considerações sobre diversos aspectos como o respeito aos dados, a

[10] "*Genetic discrimination occurs when people are treated differently by their employer or insurance company because they have a gene mutation that causes or increases the risk of an inherited disorder. Fear of discrimination is a common concern among people considering genetic testing. Several laws at the federal and state levels help protect people against genetic discrimination. In particular, a federal law called the Genetic Information Nondiscrimination Act (GINA) is designed to protect people from this form of discrimination.*"

titularidade dos dados de propriedade dos indivíduos, o tratamento de dados durante sua captação, armazenamento, processamento, uso e exclusão, além de respeitar o aspecto supranacional da circulação de informação em um mundo conectado.

No resto de sua redação, a LGPD aprofunda ainda mais o tópico, dissertando como se dá a operação dos dados, sempre norteada pelos os preceitos ditados pelo artigo 6º e seus desdobramentos.

Em respeito à exclusividade de propriedade dos dados por parte do titular a LGPD reconhece em seu artigo 17 a 22 os direitos que o titular possui sobre as suas informações, solidificando a noção de que o tratamento sobre dados só ocorre de forma correta quando esta acontece com o total consentimento daquele a quem as informações pertencem.

É também importante frisar que a partir do capítulo VI ao VIII, que contempla os artigos 37 a 54, disciplina-se os comportamentos permitidos pelos agentes que iram utilizar os dados tal como se definem boas práticas em relação ao tratamento de dados, a responsabilização legal e como ocorre a fiscalização.

Em sua parte final, a LGPD previa a criação de uma entidade nacional responsável pelo tratamento de dados, nomeada Autoridade Nacional de Proteção de Dados (ANPD) os artigos foram sumariamente vetados pelo então presidente Michael Temer (MDB) e a criação do órgão impossibilitada em primeiro instante, pois, segundo justificativa do veto, "as disposições incorrem em inconstitucionalidade do processo legislativo, por afronta ao artigo 61, § 1º, II, *e*, cumulado com o artigo 37, XIX da Constituição" (COTS & OLIVEIRA, 2018).

O veto afirma que a criação do órgão é de atribuição do Executivo, o que mais tarde foi concretizado por meio da Medida Provisória 869/18[11] (MIRANDA, 2019), reforçando ainda mais o compromisso da legislação com a proteção de dados pessoais com a criação de um órgão dedicado.

Com a edição da LGPD pode-se ver a preocupação que a proteção de dados enseja para o indivíduo moderno, é requerida uma especial atenção a este tópico para que se possam promover uma proteção completa, fato que a LGPD apresenta-se mais do que preparada em seus princípios, adequando-se as demandas atuais e relevantes, de acordo com noções modernas e se alinhando ao novo paradigma da privacidade moderna, obedecendo a sua

[11] *"A Medida Provisória (MP) 869/18, em análise no Congresso Nacional, cria a Autoridade Nacional de Proteção de Dados (ANPD). A norma foi a última editada pelo governo do ex-presidente Michel Temer.*
A criação da autoridade estava prevista na Lei de Proteção de Dados Pessoais (13.709/18). O trecho da ANPD, porém, havia sido vetado por Temer com a justificativa que a criação do órgão é prerrogativa do Executivo."

finalidade de proteção e promoção de um desenvolvimento saudável para todos os indivíduos que ela contempla.

Ainda aguardando o fim de sua *vacatio legis*, prevista para vinte e quatro meses após a sua promulgação, a LGPD é um produto da necessidade atual, sendo a sua relevância e eficácia ainda por serem postas à prova, entretanto, é possível afirmar que ela terá um ótimo desempenho em sua vigência como lei, alcançando os objetivos garantindo ao indivíduo os seus devidos direitos.

5. REFLEXÕES FINAIS

Durante a construção desta monografia foi analisado como as inovações tecnológicas e digitais influenciaram para o surgimento de um novo modo de ver a privacidade e como este fato afeta a construção da identidade humana. Em uma realidade onde o fluxo de dados cada vez mais se intensifica, não é absurdo conjecturar que a própria noção de indivíduo também passou por transformações.

O ponto crucial da analise de princípios da lei se concentrou em investigar se as novas leis que surgiram como resposta aos desafios de um mundo digital e hiperconectado baseado em uma economia de fluxo incessante de dados que, surpreendentemente, se mostrou atentos as transformações propostas pela modernidade.

A Lei de Proteção de Dados Pessoais, o Marco Civil da Internet são produtos diretos da necessidade de uma área do Direito que ainda tem muito a crescer e se transformar. Resultantes de uma preocupação fundamentada, estes dois diplomas, apesar de recentes, são essenciais para a construção de respeito a identidade e privacidade dos indivíduos e já estão preparadas para transformar a ciência jurídica de modo a aperfeiçoa-la para que produza resultados reais e pertinentes com um mundo cada vez mais conectado e complexo.

BIBLIOGRAFIA

Agência Estado. (13 de Maio de 2010). *Barreto defende criação de 'Constituição' da Internet*. Acesso em 11 de Janeiro de 2019, disponível em G1: http://g1.globo.com/brasil/noticia/2010/05/barreto-defende-criacao-de-constituicao-da-internet.html

BRASIL. (nov de 2012). Lei n. 12.737, de 30 de nov. de 2012. *Tipificação criminal de delitos informáticos* .

BRASIL. (abr de 2014). Lei n. 12.965 de 23 de abr. de 2014. *Marco civil da Internet* .

BULLA, B. (14 de Outubro de 2017). *STJ proíbe compartilhamento de dados de cartão*. Acesso em 1 de Maio de 2019, disponível em Estadão: https://economia.estadao.com.br/noticias/geral,stj-proibe-compartilhamento-de-dados-de-cartao,70002043404

BUMP, P. (19 de Março de 2018). *Everything you need to know about the Cambridge Analytica-Facebook debacle*. Acesso em 26 de Fevereiro de 2019, disponível em The Washington Post: https://www.washingtonpost.com/news/politics/wp/2018/03/19/everything-you-need-to-know-about-the-cambridge-analytica-facebook-debacle/?utm_term=.08da8f73719b

CALIXTO, D. (26 de Março de 2014). *Mídia internacional destaca pioneirismo do Brasil com Marco Civil da internet*. Acesso em 30 de Abril de 2019, disponível em Opera Mundi: https://operamundi.uol.com.br/politica-e-economia/34544/midia-internacional-destaca-pioneirismo-do-brasil-com-marco-civil-da-internet

CASTELLS, M. (2018). *O poder da identidade: a era da informação, volume 2.* São Paulo: Paz & Terra.

CAVOUKIAN, A. (Fevereiro de 2010). *Privacy by design: the 7 foundational principles - implementation and mapping of fair information practicies.* Acesso em 19 de Abril de 2019, disponível em Internet Achitecture Board: https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

COTS, M., & OLIVEIRA, R. (2018). *Lei geral de proteção de dados pessoais comentada.* São Paulo: Thomson Reuters Brasil.

FORTES, V. B. (2016). *Os direitos de privacidade e a proteção de dados pessoais na internet.* Rio de Janeiro: Lumen Juris.

FRANCIS, L. (2013). On privacy. In: J. M. ADEODATO, *Human rights and the problem of legal justice* (pp. 163-175). São Paulo: Neoses.

Genetics Home Reference. (30 de Abril de 2019). *What is genetic discrimination?* Acesso em 1 de Maio de 2019, disponível em U.S. National Library of Medicine: https://ghr.nlm.nih.gov/primer/testing/discrimination

JINKINGS, D. (24 de Agosto de 2011). *Governo apresenta proposta do Marco Civil da Internet ao Congresso Nacional*. Acesso em 27 de Março de 2019, disponível em Agência Brasil: http://memoria.ebc.com.br/agenciabrasil/noticia/2011-08-24/governo-apresenta-proposta-do-marco-civil-da-internet-ao-congresso-nacional

LEMOS, R. (22 de Maio de 2007). *Artigo: Internetbrasileira precisa de marco regulaório civil*. Acesso em 15 de Fevereiro de 2019, disponível em UOL: https://tecnologia.uol.com.br/ultnot/2007/05/22/ult4213u98.jhtm

LIMA, G. d. (2016). *Manual de direito digital: fundamentos, legislação e jurisprudência.* Curitiba: Appris.

MIRANDA, T. (3 de Janeiro de 2019). *Medida provisória cria Autoridade Nacional de Proteção de Dados*. Acesso em 25 de Março de 2019, disponível em Câmara dos Deputados: https://www2.camara.leg.br/camaranoticias/noticias/COMUNICACAO/570421-MEDIDA-PROVISORIA-CRIA-AUTORIDADE-NACIONAL-DE-PROTECAO-DE-DADOS.html

PACETE, L. G. (21 de Maio de 2018). *“A GDPR terá um efeito viral”*. Acesso em 4 de Abril de 2019, disponível em Meio & Mensagem: https://www.meioemensagem.com.br/home/midia/2018/05/21/a-gdpr-tera-um-efeito-viral.html

PEREIRA, C. M. (2010). *Instituições do direito civil* (Vol. I). Rio de Janeiro: Editora Forense.

PERIN JR., E. (Setembro de 2000). *A teoria da vontade na formação dos contratos e a autonomia do Direito Comercial em relação ao Direito Civil face ao projeto do novo Código Civil*. Acesso em 22 de Abril de 2019, disponível em jus.com.br: https://jus.com.br/artigos/518/a-teoria-da-vontade-na-formacao-dos-contratos-e-a-autonomia-do-direito-comercial-em-relacao-ao-direito-civil-face-ao-projeto-do-novo-codigo-civil

ROBL FILHO, I. N. (2010). *Direito, indimidade e vida privada.* Paraná: Juruá.

SOLOVE, D. J. (2004). *The digital person: technology and privacy in the information age.* New York: New York University Press.

STJ. (2017). *RECURSO ESPECIAL: REsp nº 1348532 / SP (2012/0210805-4). Relator: Min. Luis Felipe Saloão. DJ: 10/10/2017*. Acesso em 1 de Maio de 2019, disponível em Superior Tribunal de Justiça: https://ww2.stj.jus.br/processo/pesquisa/?src=1.1.2&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&num_registro=201202108054

TRT-3. (2018). *RECURSO ORDINÁRIO TRABALHISTA: RO 0011653-85.2017.5.03.0101. Relator: Min. Sebastião Geraldo de Oliveira. DJ 31/07/2018*. Acesso em 1 de Maio de 2019, disponível em Tribunal Regional do Trabalho da 3ª Região: https://as1.trt3.jus.br/juris/detalhe.htm?conversationId=3213

ZANINI, L. E. (2015). O surgimento e o desenvolvimento do right of privacy nos Estados Unidos. *Revista Brasileira de Direito Civil* .