CENTRO UNIVERSITÁRIO
ANTÔNIO EUFRÁSIO DE TOLEDO
DE PRESIDENTE PRUDENTE

CURSO DE DIREITO

A RESPONSABILIDADE CIVIL NA NOVA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Rafael Mitsuo Suyama Shimabukuro

PRESIDENTE PRUDENTE
2019

CENTRO UNIVERSITÁRIO
ANTÔNIO EUFRÁSIO DE TOLEDO
DE PRESIDENTE PRUDENTE

CURSO DE DIREITO

A RESPONSABILIDADE CIVIL NA NOVA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Rafael Mitsuo Suyama Shimabukuro

Monografia apresentada como requisito parcial de Conclusão de Curso para obtenção do grau de Bacharel de Direito, sob orientação do Professor Ms. Wilton Boigues Corbalar Tebar.

PRESIDENTE PRUDENTE
2019

A RESPONSABILIDADE CIVIL NA NOVA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Monografia de conclusão de Curso aprovada como requisito parcial para obtenção do grau de Bacharel em Direito.

Prof. Ms. Wilton Boigues Corbalan Tebar
Orientador

Profa. Dra. Ana Laura Teixeira Martelli Theodoro
Examinadora

Prof. Dr. Sérgio Tibiriçá Amaral
Examinador

Presidente Prudente, _____ de _____ de 2019

AGRADECIMENTOS

A princípio, agradeço a Deus por ter me dado saúde para realizar mais um projeto e sempre por ter me guiado pelo melhor caminho.

Agradeço, igualmente, aos meus pais, Célia e Pedro, por terem me dado a oportunidade de estudar sempre nas melhores instituições de ensino, e por todo apoio que me deram na realização desta pesquisa.

À faculdade, por toda sua excelência, e por disponibilizar os melhores profissionais para atender os alunos.

Ao meu Professor e Orientador Wilton Boigues Corbalan Tebar, que acreditou no meu projeto, auxiliou-me nas pesquisas e sempre me motivou a escrever mais.

Aos meus caros amigos da 2ª Promotoria de Justiça de Presidente Prudente, que me incentivaram e me ajudaram a escrever esta monografia, além de me proporcionarem bons aprendizados.

Por fim, mas não menos importante, agradeço aos meus amigos que, diariamente, estão comigo me aconselhando e me apoiando.

RESUMO

O presente trabalho tem como principal objetivo estudar acerca da responsabilidade civil na Lei Geral de Proteção de Dados Pessoais, contudo, também tem como foco demonstrar a importância do direito a proteção de dados pessoais como um direito personalíssimo diverso do direito à privacidade, e se este tem amparo constitucional. Para tanto, é necessário trabalhar o conceito de “dados pessoais”, a evolução histórica da proteção destes dados, os fenômenos da datificação, do *proffiling* e claramente um estudo direcionado acerca das constituições que amparam o direito a proteção de dados pessoais. Utiliza-se o método cientifico dedutivo, fundado em estudos histórico, jurisprudencial, legal, doutrinário e posteriormente é feito um breve estudo de casos para tecer as conclusões do trabalho.

Palavras-chave: Direito Civil. Direito do Consumidor. Lei Geral de Proteção de Dados Pessoais. Responsabilidade Civil.

ABSTRACT

The present work has as main objective to study about the civil liability in the General Personal Data Protection Act, however, it also has as focus to demonstrate the importance of the right to protection of personal data as a very personal right different from the right to privacy, and if this must have constitutional protection. To this end, it is necessary to work on the concept of “personal data” and the historical evolution of data protection, the phenomena of datification and profiling and clearly a directed study about the constitutions that support the right to protection of personal data. The deductive scientific method, based on historical, jurisprudential, legal, doctrinal, and then a brief of situational studies is used to weave the conclusions of the work.

Key words: Civil Right. Consumer Law. General Personal Data Protection Act. Civil Liability.

SUMÁRIO

1 INTRODUÇÃO

Com os avanços tecnológicos e com a globalização, a população se viu mais conectada do que nunca, era possível conversar com qualquer pessoa no globo terrestre sem nenhuma dificuldade, bastando para tal, acesso à *internet*.

Contudo, o avanço tecnológico traz as suas desvantagens, uma das principais era a privacidade dos usuários na rede. Com a grande divulgação de informação *online,* diferenciar o que estava na esfera da privacidade e da publicidade se tornou uma tarefa difícil, tanto é que foi alvo de vários estudos.

O grande ponto é que na medida em que a população foi se computadorizando, muitas informações pessoais foram jogadas na rede, tais informações que geralmente são utilizadas por grandes empresas para manipular as massas.

Partindo deste pressuposto era extremamente importante que os usuários estivessem atentos a qualquer coleta de dados, pois era direito dos mesmos que fossem informados quando seus dados estivessem sendo coletados e para quais fins os mesmos estavam sendo utilizados.

Nesse sentido, o presente trabalho visou abordar um dos temas que se tornou gritante após as eleições presidenciais dos Estados Unidos, e a responsabilidade do tratamento irregular dos dados pessoais.

Dessa forma, no primeiro capítulo foi estudado acerca dos dados pessoais, trabalhando o conceito deste e a evolução da sua proteção, além de deixar claro uma nova vulnerabilidade do cidadão. Também foi abordando os meios de mineração e os agentes envolvidos no tratamento de dados pessoais.

Posteriormente, no segundo capítulo, buscou-se trabalhar a proteção de dados pessoais como um direito fundamental, para tanto foi necessário abranger temas como a biografia digital, autodeterminação informacional e diferenciar o direito à proteção de dados pessoais do direito à privacidade.

Por fim, o último capítulo destinou-se exclusivamente à lei 13.709 de 2018, utilizou-se os conhecimentos trabalhados nos capítulos anteriores e métodos de hermenêutica, para tecer as obrigações dos agentes de tratamento de dados.

Para a elaboração deste trabalho foi utilizado o método dedutivo, pautando-se na interpretação de leis nacionais e internacionais, também sendo

utilizado a doutrina e jurisprudência. Ademais, após uma análise doutrinária, jurisprudência e legal, foi possível extrair diversas conclusões acerca do tema.

2 DOS DADOS PESSOAIS

Para uma melhor análise do tema é necessário, a princípio, estudarmos acerca do contexto histórico dos dados pessoais e das leis de proteção, os conceitos adotados pelos diplomas legais de outros países, bem como o adotado no ordenamento brasileiro, e por fim, estabelecer a sua importância na sociedade contemporânea.

2.1 Breve Contexto Histórico Da Proteção De Dados

Graças a corrida tecnológica e ideológica travada entre os Estados Unidos e a União Soviética, muitas tecnologias foram inventadas ou aperfeiçoadas, dentre as quais está a "*Arpanet*". Assim, em 1969, nos Estados Unidos, surgia o que chamamos hoje de *internet*.

Inicialmente a "*Arpanet*" tinha como principal função estabelecer uma comunicação segura, sendo utilizada mais como uma "[...] garantia de que a comunicação entre militares e cientistas persistiria, mesmo em caso de bombardeio" (SILVA, 2001, s.p).

Atualmente a *internet* serve principalmente como um meio de difusão de informações, além de ter se transformado em um forte instrumento de engajamento social:

> Um exemplo sintomático foram as manifestações de junho de 2013. Nelas, o exercício de cidadania foi revitalizado por um fluxo informacional – em especial as redes sociais – que conectou seus manifestantes, facilitando a organização e a disseminação dos protestos. Verificou-se, sobretudo, um novo instrumento de engajamento social (BIONI, 2019, p. 05).

A *internet* possui inúmeras outras utilidades, entre as quais, está um dos objetos centrais do presente trabalho, a obtenção ou "mineração"[1] de dados pessoais.

Com o conhecimento dos dados pessoais "[...] a ciência mercadológica percebeu que a Internet poderia propiciar uma abordagem publicitária mais efetiva." (BIONI, 2019, p. 18), dessa maneira tais dados passaram a serem utilizados de maneiras indevidas e muitas vezes sem o consentimento dos seus titulares.

---

[1] Termo utilizado por Bruno Bioni (2019).

Observando a situação, vários Estados começaram a regulamentar a obtenção e utilização dos dados pessoais, o que dá início às gerações de leis de proteção dos dados pessoais.

Na primeira geração, buscou-se “regular um cenário no qual centros elaboradores de dados, de grande porte, concentrariam a coleta e gestão dos dados pessoais.” (DONEDA, 2011, p. 96) e “(...)o controle do uso de informações pessoais pelo Estado e pelas suas estruturas administrativas (...)” (Ibidem).

Segundo Viktor Mayer-Schönberger, a primeira geração de leis não focava na proteção direta e individual do direito à privacidade, mas sim na “função do processamento de dados na sociedade”:

> Most of the first-generation data-protection norms do not focus on the direct protection of individual privacy. Instead they concentrate on the function of individual privacy. [2] (MAYER-SCHÖNBERGER, 2001, p. 223)

Ainda sobre o tema, o autor cita que: “[…] the first-generation data-protection norms take a functional look at the phenomenon of data processing”[3] (MAYER-SCHÖNBERGER, 2001, p. 223), devido a este olhar funcional muitos indivíduos não poderiam escolher onde poderiam processar os seus dados: “Individuals could not decide whether their data was at all”[4] (MAYER-SCHÖNBERGER, 2001, p. 226).

Laura Schertel dá bons exemplos de leis desta geração:

> São exemplos de normas da primeira geração as leis do Estado alemão de Hesse (1970), a Lei de Dados da Suécia (1973), o Estatuto de Proteção de Dados do Estado alemão de Rheinland-Pfalz (1974) e a Lei Federal de Proteção de Dados da Alemanha (1977). (MENDES, 2014 apud MAYER-SCHÖNBERGER, 2001, p. 221)

Há de se destacar que Portugal foi um dos primeiros Estados a constitucionalizar o direito a proteção de dados, prevendo em sua carta magna o direito de todos os cidadãos de tomar conhecimento de constar em registros “mecanográficos”: “[...] daí a constitucionalização da Proteção de Dados: em Portugal

[2] A maior parte das normas da primeira geração de leis de proteção de dados não focavam na proteção direta e individual da privacidade. Ao invés, focavam na função do processamento de dados na sociedade (tradução nossa).
[3] As normas de primeira geração têm um olhar funcional sobre o fenômeno do processamento de dados (tradução nossa).
[4] As pessoas não podiam decidir onde seus dados eram processados (Tradução nossa).

(Art.º 35.º da Constituição da República Portuguesa), desde 1976." (MASSENO, 2018, p. 03).

Além disso a Constituição Portuguesa já previa um pequeno rol de dados pessoais que não poderiam ser tratados pela informática, tal rol, inclusive, inclui vários exemplos de dados sensíveis:

> 1. Todos os cidadãos tem o direito de tomar conhecimento do que constar de registos mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir a rectificação dos dados e a sua actualização.
> 2. A informática não pode ser usada para tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se trate do processamento de dados não identificáveis para fins estatísticos.
> 3. É proibida a atribuição de um número nacional único aos cidadãos. (PORTUGAL, 1976)

Contudo, tais leis se mostraram genéricas e amplas demais, isso graças a "[...] a falta de experiência no tratamento com tecnologias ainda pouco familiares, aliada ao receio de um uso indiscriminado dessa tecnologia, sem que se soubesse ao certo suas consequências [...]" (DONEDA, 2011, p. 96, apud Spiros Simitis, 1997, p. 565), ademais, a coleta e gestão de dados não se limitou tão somente aos órgãos do Estado, fato que "[...] aumentou a quantidade de atores e, simetricamente, o número de bancos de dados a serem regulados-autorizados. Esse novo cenário exigiu uma nova estrutura normativa." (BIONI, 2019, p. 114).

O que nos leva ao final da década de 1970, com o surgimento das leis de segunda geração. Tais leis tinham como principal característica a sua abrangência às relações privadas:

> O que era exceção veio a se tornar regra. Tanto o Estado quanto os entes privados utilizavam intensamente o fluxo de informações pessoais para seu funcionamento, e a interrupção ou mesmo o questionamento deste fluxo pelo cidadão implica muito frequentemente a sua exclusão de algum aspecto da vida social. (DONEDA, 2011, p. 97).

Esta geração também poderia ser caracterizada por considerar a proteção de dados pessoais como uma "liberdade negativa, a ser exercitada pelo próprio cidadão" (DONEDA, 2006, p. 209). Desta forma, conclui Bioni:

> [...] A segunda geração de leis transfere para o próprio titular dos dados a responsabilidade de protege-los. Se antes o fluxo das informações pessoais deveria ser autorizado pelo Estado, agora cabe ao próprio cidadão tal ingerência que, por meio do consentimento, estabelece as suas escolhas no

> tocante à coleta, uso e compartilhamento dos seus dados pessoais. (BIONI, 2019, p. 115, apud MAYER-SCHÖNBERGER, 2001, p. 226-227)

Assim, nesta geração o foco principal era no direito à privacidade, ao invés dos procedimentos: “Tais normas buscavam tratar prioritariamente do direito à privacidade, em vez de procedimentos.” (MENDES, 2014, s.p), pode-se dizer que em partes é o inverso da primeira geração.

Podemos citar como exemplos de leis da segunda geração: “[...] a Lei Francesa de Proteção de Dados Pessoais de 1978, intitulada *Informatique et Libertées*, além da já mencionada Bundesdatenschutzgesetz” (DONEDA, 2011, p. 97).

Todavia, esta geração foi gravada por falhas graves, uma delas foi individualizar a proteção de dados que consequentemente permitia ao cidadão interromper, quando quiser, o fluxo de seus dados, contudo, tal possibilidade poderia exclui-lo de algum aspecto de sua vida social:

> Por um lado, no âmbito do Estado Social, é muito difícil assegurar-se a liberdade informacional sem comprometer as funções dessa complexa burocracia que necessita de dados dos cidadãos para planificar. Por outro, também na relação entre privados é difícil se verificar o exercício do direito à privacidade informacional, na medida em que tal exercício poderá impedir o acesso do indivíduo a determinadas facilidades do mercado de consumo, que o fornecedor está disposto a conceder somente em troca de suas informações pessoais. (MENDES, 2014, s.p)

Ainda:

> Enfim, percebia-se que o exercício puramente individual desta liberdade envolvia consequências bem maiores que aquelas que diziam respeito somente às informações pessoais e que eram fundamentais para a própria socialização de cada pessoa. (DONEDA, 2006, p. 211)

Doneda e os demais autores, baseiam suas críticas à segunda geração nos comentários de Viktor Mayer-Schönberger:

> A proteção de dados pessoais como liberdade individual pode proteger a liberdade do indivíduo. Ela pode oferecer ao indivíduo a possibilidade de não conceder informações a seu respeito que lhe são solicitadas. Mas qual será o custo que se tem de pagar por isso? É aceitável que a proteção de dados pessoais possa ser exercida apenas por eremitas? (MENDES, 2014, *apud* MAYER-SCHÖNBERGER, 2001, p. 228, tradução da autora)

Na década de 1980 surgiu a terceira geração de leis de proteção de dados pessoais, o qual é “[...] marcada pela decisão do Tribunal Constitucional alemão

, de 1983, que declarou a inconstitucionalidade de parte da Lei do Censo.” (MENDES, 2014, s.p).

O julgado do Tribunal Alemão foi fundamental para o estabelecimento do direito à autodeterminação informativa[5]:

> [...] o grande mérito do julgamento reside na consolidação da ideia de que a proteção de dados pessoais baseia-se em um direito subjetivo fundamental, que deve ser concretizado pelo legislador e que não pode ter o seu núcleo fundamental violado. Isso significa uma limitação ao poder legislativo, que passa a estar vinculado à configuração de um direito à autodeterminação da informação. (MENDES, 2011, p. 04)

Uma das consequências do julgado foi a difusão do direito a autodeterminação informativa pela Europa: “[...] seguiram-se emendas às leis de proteção de dados pessoais na Alemanha e na Áustria, além de leis específicas na Noruega e na Finlândia” (DONEDA, 2006, p. 211).

Ademais, a terceira geração ficou caracterizada pela participação do cidadão no processo de obtenção e difusão dos seus dados:

> [...] participação do cidadão no processamento de seus dados passa a ser compreendida como um envolvimento contínuo em todo o processo, desde a coleta, o armazenamento e a transmissão e não apenas como a opção entre “tudo ou nada”. (MENDES, 2014, s.p)

Buscou-se uma participação maior dos cidadãos, por meio da autodeterminação informativa, todavia, com o tempo, percebeu-se que poucas pessoas estavam exercendo suas prerrogativas, tornando assim, um privilégio de poucos:

> As leis de terceira geração encaravam a participação do cidadão como uma mola propulsora de sua estrutura. Percebeu-se, no entanto, que na realidade não seriam muitas as pessoas dispostas a exercitas suas prerrogativas, dado que os custos envolvidos, sejam eles econômicos ou sociais, geralmente as compeliam a aquiescer com situações que não eram as ideias. A autodeterminação informativa, portanto, continuava sendo o privilégio de uma minoria que decidia enfrentar tais custos. (DONEDA, 2006, p. 212)

Podemos perceber que alguns dos defeitos da segunda geração ainda persistiram, principalmente o fato do exercício do direito a proteção de dados ser

[5] Este tema será estudado mais a fundo no tópico 3.2

dificultado pela possibilidade de o indivíduo ser excluído de alguns aspectos da vida social.

A quarta geração, marcada pelas leis atuais, tem como objetivo principal tentar "[...] suprir as desvantagens do enfoque individual existente até então" (DONEDA, 2006, p. 212).

Nesse liame, observa-se dois meios para atingir essa meta: "Primeiramente, algumas das normas visaram fortalecer a posição dos indivíduos, tornando mais efetivo o seu autocontrole sobre os dados pessoais." (MENDES, 2014, s.p), nesse caso, podemos observar mudanças normativas mundiais:

> [...] For example, recent amendments to German states' data-protection laws, and the German Federal Data Protection Statute of 1990, introduced no-fault compensation for individual data-protection claims.[6] (MAYER-SCHÖNBERGER, 2001, p. 233)

Outra dessas mudanças, é a supressão de temas complexos da abrangência do controle individual, leva-se em consideração a (hyper) vulnerabilidade do consumidor frente aos seus dados pessoais:

> [...] as normas retiraram da esfera do controle do indivíduo determinados assuntos, por compreenderem que alguns temas relativos aos dados pessoais são tão relevantes para o cidadão que merecem ser extremamente protegidos, não podendo estar na esfera de disposição individual. (MENDES, 2014, s.p).

A segunda medida foi a criação de autoridades independentes para a aplicação das leis de proteção de dados pessoais, além do surgimento de mais normas setoriais que complementavam as normas gerais:

> Outras características são a disseminação do modelo das autoridades independentemente para a atuação da lei – tanto mais necessárias como a diminuição do poder de "barganhar" do indivíduo para a autorização ao processamento de seus dados, e também o surgimento de uma normativa conexa tal como as normas especificas para alguns setores de processamento de dados (por exemplo, para o setor de saúde ou de crédito ao consumo). (DONEDA, 2006, p. 213).

[6] Por exemplo, as recentes emendas às Leis de Proteção de Dados Estaduais Alemãs e a Lei Federal Alemã de Proteção de Dados Pessoais, estatuto de 1990, introduziram o "*no-fault* compensation" para as reclamações individuais... (tradução nossa).

Um exemplo recente de dispositivo dessa geração é o Regulamento Geral sobre a Proteção de Dados (RGPD), que trouxe vários direitos aos cidadãos que incluem:

> [...] um consentimento claro e positivo do tratamento dos seus dados e o direito de receber informações claras e compreensíveis sobre o mesmo; o direito a ser esquecido — um cidadão pode solicitar que os seus dados sejam suprimidos; o direito a transferir os dados para outro prestador de serviços (por exemplo, a mudança de uma rede social para outra); e o direito de saber se os seus dados foram pirateados. (PROTEÇÃO dos dados pessoais).

Dessa forma findamos o nosso breve contexto histórico acerca da Proteção de Dados, o que nos permite partir para os estudos acerca dos conceitos de dados pessoais adotados pela grande parte dos diplomas mundiais.

2.2 O Que São Dados Pessoais?

A conceituação de “dados pessoais” é elemento central de qualquer trabalho, tendo em vista que “Não seria qualquer dado que teria repercussão jurídica, mas, somente, aquele que atraísse o qualificador pessoal” (BIONI, 2019, p. 68).

Dessa forma, estaremos analisando os conceitos utilizados pelos diplomas de outros Estados, bem como o utilizado pela Lei Geral de Proteção de Dados Pessoais (LGPD) e principalmente aprofundar nosso estudo nas teorias existentes sobre o conceito de dados pessoais.

Porém, cabe antes mencionar os conceitos atribuídos ao termo “dados pessoais” pelos dicionários mais tradicionais: “11 informação relativa a um indivíduo, capaz de identifica-lo<d. pessoais>” (HOUAISS, 2001, p.903); “Personal [...] Belonging to or affecting a particular person rather than anyone else.” [7] (OXFORD, 2019, s.p) e “Data […] Facts and statistics collected together for references or analysis”[8] (Ibidem).

Diante dos conceitos extraídos dos dicionários podemos chegar a um primeiro resultado, sendo dado pessoal aquele que é referente ou pertencente à uma pessoa já identificada ou que poderá ser identificada, tal conceito se aproxima muito do conceito adotado pela teoria expansionista, o qual estaremos estudando adiante.

---

[7] Pessoal [...] (algo)pertencente ou afeto a uma pessoa mais que qualquer outra (tradução nossa)
[8] Dados [...] fatos e estatísticas coletados juntos para referencias ou analises (tradução nossa)

2.2.1 Conceito reducionista *versus* expansionista

Quanto ao conceito dos dados pessoais há duas grandes correntes que foram adotados pelos diplomas legais mundiais, a reducionista e a expansionista: “Information privacy law is now divided between reductionist and expansionist regulation of PII.”[9] (SCHWARTZ Paul M; SOLOVE, Daniel J, 2011, p. 1872). A adoção de uma teoria ou outra gera grandes efeitos no âmbito da proteção de dados, conforme veremos adiante.

Na perspectiva reducionista os dados pessoais devem “estar associados a uma pessoa especifica” (BIONI, 2015, p.21), assim, para essa teoria um dado pessoal deve identificar um sujeito especifico: “[...] only to information that taken in isolation, in that single case, actually identifies a specific individual. We will call this viewpoint the ‘reductionist reading’ of PII.”[10] (SCHWARTZ Paul M; SOLOVE, Daniel J, 2011, p. 1870-1871).

Um dos poucos países que adotaram esta teoria foi os Estados Unidos, por meio do “Privacy Act of 1974” que graças a sua definição de registro, tal lei não é aplicada aos casos em que há um dado que não identifica um indivíduo “único”:

> Another example of the reductionist tendency in the United States involves the Privacy Act's definition of a "system of records," which turns on whether federal agency records involve an "identified" person. The Privacy Act does not apply to data processing if a person is identifiable within a federal agency's database, but is not located through a unique identifier.[11](SCHWARTZ Paul M; SOLOVE, Daniel J, 2011, p. 1873).

Diante desse conceito reducionista, percebeu-se uma falha: se os dados pessoais são aqueles que inequivocamente identificam uma pessoa, os dados que potencialmente poderiam identificar esta mesma pessoa também não se enquadrariam como dados pessoais e não merecem a mesma proteção?

---

[9] As leis de privacidade de informação estão, agora, divididas em regulamentações reducionistas e expansionistas do PII (tradução nossa).

[10] [...] somente para informações que tomado isoladamente, num caso único, identifica um indivíduo específico. Nós chamaremos este ponto de vista de “reducionist reading” do PII.

[11] Outro exemplo da tendência reducionista nos Estados Unidos envolve a definição da Lei de Privacidade de um "sistema de registros", que gira em torno do fato de os registros da agência federal envolverem uma pessoa "identificada". A Lei de Privacidade não se aplica ao processamento de dados se uma pessoa é identificável dentro do banco de dados de uma agência federal, mas não é localizada através de um identificador único. (Tradução Nossa).

Tomemos por exemplo um banco de dados de alunos de uma determinada escola. Neste banco há quatro informações de todos os alunos: 1) o nome; 2) número escolar; 3) classe que estuda e 4) endereço de residência. Para a teoria reducionista somente o número escolar (que em tese deve ser único para cada aluno) tratar-se-ia de um dado pessoal, já que é possível haver alunos homônimos, haver mais de um aluno em uma classe e/ou haver mais de uma pessoa morando no endereço indicado.

Nesse sentido somente o número escolar dos alunos seria abrangido pela proteção da lei, enquanto o nome, classe e endereço não. Entretanto, ainda continua sendo possível identificar a pessoa com estas informações.

O exemplo citado é algo simplório, tendo em vista que atualmente há vários meios de transformar os dados em "anônimos", todavia, conforme mostra o caso *Netflix Prize*[12], ficou evidente que, da mesma forma que há vários métodos para tornar os dados anônimos, há meios tão eficazes quanto, para torna-los identificáveis:

> We have presented a de-anonymization methodology for sparse micro-data, and demonstrated its practical applicability by showing how to de-anonymize movie viewing records released in the Netflix Prize dataset. Our de-anonymization algorithm Scoreboard RH works under very general assumptions about the distribution from which the data are drawn, and is robust to data perturbation and mistakes in the adversary's knowledge. Therefore, we expect that it can be successfully used against any dataset containing anonymous multi-dimensional records such as individual transactions, preferences, and so on[13].(NARAYANAN, Arvind; SHMATIKOV, Vitaly, sem data, p. 13-14)

Se não bastasse, há outros dois casos que merecem destaque, o primeiro é o método demonstrado por Latanya Sweeney, que em seu estudo revelou ser possível identificar cerca de oitenta e sete por cento dos norte-americanos, levando em consideração somente três fatores: "It was found that 87% (216 million of 248 million) of the population in the United States had reported characteristics that likely

[12] Foi um evento promovido pela *streaming* Netflix em que "[...] a Netflix disponibilizou a sua base de dados com todas as avaliações de seu catalogo de filmes do período de 1998 e 2005, suprimindo nomes dos usuários e deixando somente a data e a nota da avaliação" (BIONI, 2019, p. 73) no intuito de melhorar o seu algoritmo de sugestão de filmes.

[13] Apresentamos uma metodologia de "desanonimar" microdados esparsos e demonstramos sua aplicabilidade prática mostrando como "desanonimar" os registros de visualização de filmes lançados no conjunto de dados do Netflix Prize. Nosso "ScoreboardRH de-anonymizationalgorithm" trabalha sob hipóteses muito gerais sobre a distribuição da qual os dados são extraídos, e é robusto para perturbação de dados e erros no conhecimento do adversário. Portanto, esperamos que ele possa ser usado com êxito contra qualquer conjunto de dados que contenha registros multidimensionais anônimos, como transações individuais, preferências e assim por diante. (tradução nossa).

made them unique based only on {5-digit ZIP, gender, date of birth}"[14] (SWEENY, 2000, p. 2).

O segundo, envolve um portal norte-americano chamado AOL, que reuniu informações acerca das centenas de pesquisas e cliques em sua página online de um determinado usuário (identificado como nº 4417749), conseguindo assim traçar um parâmetro e identificar este usuário:

> No. 4417749 conducted hundreds of searches over a three-month period on topics ranging from "numb fingers" to "60 single men" to "dog that urinates on everything." And search by search, click by click, the identity of AOL user No. 4417749 became easier to discern. There are queries for "landscapers in Lilburn, Ga," several people with the last name Arnold and "homes sold in shadow lake subdivision gwinnett county georgia."It did not take much investigating to follow that data trail to Thelma Arnold, a 62-year-old widow who lives in Lilburn, Ga., frequently researches her friends' medical ailments and loves her three dogs.[15] (BARBARO e ZELLER Jr, 2006, s.p).

Nesse sentido percebe-se que somente a proteção dos dados atrelados a pessoas identificadas já não é o suficiente, dessa forma a teoria expansionista sana o problema apresentado pela teoria anterior acrescentando ao conceito o termo "identificável":

> Enquanto que a expansionista aposta em uma lógica mais flexível que desconsidera a associação exata entre uma informação e uma pessoa. Dado pessoal pode ser qualquer tipo de informação que permita a sua identificação, ainda que o vínculo entre o dado e um indivíduo não seja estabelecido de prontidão, mas de forma mediata ou indireta. Um dado para ser pessoal deve ser, portanto, a projeção de uma pessoa identificável. (BIONI, 2015, p. 17)

O primeiro documento legal que seguiu a corrente expansionista foi a *Bundesdatenschutzgesetz*, lei alemã de 1977, que definiu dados pessoais como informações relacionadas tanto a indivíduos identificados e identificáveis:

---

[14] Verificou-se que 87% (216 milhões de 248 milhões) da população nos Estados Unidos relataram características que provavelmente os tornaram únicos com base apenas no {Código Postal de 5 dígitos, sexo, data de nascimento} (Tradução Nossa)

[15] Nº 4417749 realizou centenas de buscas durante um período de três meses em tópicos que variavam de "dedos dormentes" a "homens de 60 anos solteiros" a "cachorro que urina em tudo". E procura por pesquisa, clique por clique, a identidade do usuário AOL Nº. 4417749 tornou-se mais fácil de discernir. Há perguntas para "paisagistas em Lilburn, Ga", várias pessoas com o sobrenome Arnold e "casas vendidas na subdivisão do lago das sombras em gwinnett county georgia". Não foi preciso muita investigação para seguir essa trilha de dados para Thelma Arnold, uma viúva de um ano que mora em Lilburn, Geórgia, frequentemente pesquisa os problemas médicos de seus amigos e ama seus três cachorros. (Tradução Nossa).

> The treatment in privacy of identified and identifiable as equivalents is a German innovation. The German Federal Data Protection Act (Bundesdatenschutzgesetz, or BDSG) of 1977 defines "personal data" information as data relating to both "identified" and "identifiable" individuals.[16] (SCHWARTZ Paul M; SOLOVE, Daniel J, 2011, p. 1874)

Ainda:

> 1. ‘personal data’ means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;[17] (ALEMANHA, 2017, Part. I, Capitulo I, Seção 46)

Vários outros Estados e organizações adotaram esta teoria, como a OECD (The Organisation for Economic Co-operation and Development), que também define dados pessoais como: “[…] any information relating to an identified or identifiable individual (data subject)”[18] (OECD Guidelines,2013), em sentido semelhante há as leis do Canada[19], Argentina[20], APEC[21] (Asia-Pacific Economic Cooperation), Brasil[22], Europa[23] entre outros.

Contudo, houve grandes críticas aos diplomas europeus que determinaram que os termos “identificado” e “identificável” são equivalentes, já que por vezes, tornar dados anônimos em identificados podia dispender níveis de esforço (tempo e recursos) diferentes:

> Notwithstanding its widespread adoption in other international documents, the European Union's expansionist approach is flawed because it treats data about identifiable and identified persons as conceptually equivalent. The difficulty is that there is a broad continuum of identifiable information that includes different kinds of anonymous or pseudonymous information. Different

---

[16] O tratamento na privacidade de equiparar identificável e identificado é uma inovação alemã. A lei federal de proteção de dados (*Bundesdatenschutzgesetz* ou BDSG) de 1977 define “dado pessoal” como um dado relacionado tanto a indivíduos “identificados” quanto “identificáveis”. (tradução nossa).
[17] ‘dados pessoais’: significa qualquer informação relacionada a uma pessoa natural identificada ou identificável (assunto dos dados); uma pessoa natural identificável é aquela que pode ser identificada, diretamente ou indiretamente; em particular por referencias de um identificador como um nome, número de identificação, dados de localização, um identificador online ou um ou mais fatores específicos de identidades físicas, psicológicas, mentais, econômicas, culturais ou sociais daquela pessoa; (tradução nossa).
[18] [...] qualquer informação relacionada a uma pessoa identificada ou identificável (tradução nossa)
[19] Personal Information Protection and Eletronic Document Act (PIPEDA), S.C. 2000, c.5 (section 2).
[20] Leyi 25.326 de 30 de outubro de 2000, articulo 2º.
[21] APEC Privacy Framework, part. II scope, Definitions.
[22] Lei nº 13.709, de 14 de agosto de 2018, art. 5º, I.
[23] Artigo 4º, nº 1, da GDPR (*General Data Protection Regulamentation)*

> levels of effort will be required to identify information, and varying risks are associated with the possible identification of data. To place all such data into the same conceptual category as data that currently relate to an identified person is a blunt approach.[24] (SCHWARTZ Paul M; SOLOVE, Daniel J, 2011, p. 1876)

Além disso, diante da interpretação literal da teoria expansionista, junto ao avanço das técnicas de "desanonimização" uma informação, poderíamos considerar que todos os dados seriam identificáveis:

> [...] Do contrário, repita-se, haveria uma redundância normativa, na medida em que dados anônimos sem o critério da razoabilidade – seriam sempre enquadrados dentro do conceito de dado pessoal, como aquele relacionado a uma pessoa identificável. (BIONI, 2019, p. 77).

Devido a esse fator, o critério da razoabilidade foi importante para delimitar o que viria a ser dados pessoais. A grande questão agora é saber qual a abrangência do razoável, principalmente na Lei Geral de Proteção de Dados.

2.2.1 Aplicação Do Princípio da Razoabilidade Para Os Dados Identificáveis

Conforme demonstrado no final do subtópico anterior não são todos os dados identificáveis que são abrangidos pelo conceito de dado pessoal, portanto, precisou-se delimitar o que vem a ser um dado identificável.

Tal delimitação, nos diplomas Europeus, valeu-se do critério da dificuldade da identificação de determinados dados anônimos, ou seja, dependendo do nível de dificuldade e recursos gastos para tornar o dado identificável, ele não estaria englobado no conceito de dado pessoal, logo, não estaria sob a proteção da lei:

> [...] o direito comunitário europeu e a LGPD valeram-se do critério da razoabilidade para delimitar o espectro do conceito expansionista de dados pessoais. Não basta a mera possibilidade de que um dado seja atrelado a uma pessoa para atrair o termo de identificável. Essa vinculação deve ser

[24] Apesar de sua ampla adoção em outros documentos internacionais, a abordagem expansionista da União Européia é falha porque trata os dados sobre pessoas identificáveis e identificadas como conceitualmente equivalentes. A dificuldade é que existe um amplo continum de informações identificáveis que inclui diferentes tipos de informações anônimas ou sob pseudônimos. Diferentes níveis de esforço serão necessários para identificar informações, e vários riscos estão associados à possível identificação de dados. Colocar todos esses dados na mesma categoria conceitual dos dados que atualmente se relacionam com uma pessoa identificada é uma abordagem erronea. (Tradução nossa)

> objeto de um “esforço razoável”, sendo esse o perímetro de elasticidade do conceito de dado pessoal como aquele relacionado a uma pessoa identificável (BIONI, 2019, p. 76).

A *General Data Protectio Regulamentation* da União Europeia reforça o argumento, já que em seu considerando 26 menciona a razoabilidade nos meios de “desanonimizar” um dado pessoal, inclusive complementando os critérios para identificar um “meio razoável”:

> (26) Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica. (EUROPA, 2016, considerando 26).

Já a Lei Geral de Proteção de Dados Pessoais brasileira prevê o princípio em seu artigo 12 §1º:

> Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.
> § 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios. (BRASIL, 2019, art. 12)

Os dados anônimos citado pelo artigo são aqueles relativos aos titulares que, em teoria, não podem ser identificados:

> 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; (BRASIL, 2019, art. 5º)

Tal dispositivo serve principalmente para evitar uma redundância normativa, na medida em que distingue o que são considerados dados pessoais e dados anônimos:

> [...] dados anônimos – sem o critério da razoabilidade – seriam sempre enquadrados dentro do conceito de dado pessoal, com aquele relacionado a uma pessoa identificável (BIONI, 2019, p. 77)

Percebe-se que o artigo 12 da LGPD se espelhou no considerando 26 da GDPR, aliás vários outros dispositivos da lei brasileira se assemelham aos europeus.

Dessa forma, podemos entender como razoável, o esforço que leva um tempo e gastos médios para desanonimar um dado pessoal, para assim este se enquadrar no conceito de dados pessoais.

Diante de todo o exposto podemos conceituar dado pessoal como, uma informação atrelada à uma pessoa já identificada ou que é identificável pelos métodos que são considerados como razoáveis, o qual merece proteção jurídica.

2.3 A Importância Dos Dados Pessoais e a Nova Vulnerabilidade Do Cidadão

Na sociedade atual a informação se tornou um elemento fundamental para o sucesso ou fracasso de projetos, basta o conhecimento desconhecimento de um elemento para comprometer uma investida na bolsa de valores, por exemplo.

Não é à toa que muitos consideram a informação como um “elemento estruturante que (re) organiza a sociedade, tal como o fizeram a terra, as máquinas a vapor e a eletricidade [...]” (BIONI, 2019, p.05), ou seja, uma nova espécie de “matéria-prima”. Portanto, em um primeiro momento podemos dizer que a informação é a matéria bruta dessa revolução.

Entretanto, não poderíamos dizer que a “simples” informação “bruta” seria o grande diferencial em um mercado por exemplo. Deve-se levar em consideração a aplicação dessa informação na geração de novos conhecimentos e demais inovações:

> O que caracteriza a atual revolução tecnológica não é a centralidade de conhecimento e informação, mas aplicação desses conhecimentos e dessa informação para a geração de conhecimentos e de dispositivos de processamento/comunicação da informação, em um ciclo de realimentação cumulativo entre a inovação e seu uso (CASTELLS, 2006, p. 69)

Diante dessa nova concepção podemos dizer que a informação é a matéria bruta, porém, a transformação dessas informações em lucros ou vantagens é o fundamental nesta “sociedade da informação”.

Dentro de uma sociedade que é movida por informações, ter o conhecimento do que as pessoas gostam, compram, conversam etc... se tornou

fundamental para qualquer tipo de projeto, desde uma simples proposta de marketing até uma campanha política.

É nesse contexto que os dados pessoais se destacam, atualmente grande parte das informações sobre as pessoas são armazenadas em bancos de dados, sendo utilizados muitas vezes para traçar estratégias de marketing, pode-se dizer que grande parte dos dados pessoais ou não pessoais, tornaram-se uma matéria prima de negócios:

> Data was no longer regarded as static or stale, whose usefulness was finished once the purpose for which it was collected was achieved […] Rather, data became a raw material of business, a vital economic input, used to create a new form of economic value.[25] (MAYER-SCHONEBERGER, Viktor; CUKIER, Kenneth, 2013, p. 05).

Ora, um grande exemplo da grande importância dos dados pessoais, está na recente compra do aplicativo de celular “WhatsApp” pelo “Facebook”. Um dos grandes motivos dessa compra foi justamente os dados pessoais dos usuários do “WhatsApp”, que passaram a ser utilizados para incrementar a publicidade comportamental do “Facebook”:

> [...] À época a conta que se fez foi prospectar como possivelmente Zuckerberg monetizaria os dados da audiência do aplicativo por meio de publicidade comportamental [...] A nova política de privacidade do WhatsApp concretiza a cogitada reversão do seu modelo de negócio. Agora os dados dos seus usuários serão compartilhados entre “a Família de Empresas do Facebook” para aprimorar “as experiências” dos seus serviços, em particular com relação a “anúncios e produtos no Facebook”. (BIONI, 2016, s.p)

Interessante notar que inicialmente o “WhatsApp” tinha a proposta de ser um “veículo de mensagens” ao mesmo tempo que preserva os dados pessoais dos usuários, com a venda do aplicativo ao “Facebook” tal ideia é descartada:

> O WhatsApp foi criado com a promessa de que os nossos “dados não estariam na jogada”. Esse foi o termo utilizado pelos seus fundadores que eram refratários à lógica do chamado zero-price-advertisement-bussiness. Ou seja, eles apostavam na ideia de que os usuários pagariam o valor de US$1,00 (um) dólar por ano, ao invés dos seus dados serem a moeda de troca pelo serviço. Tanto que chegaram a vocalizar o coro de que “quando há anúncios, você, o usuário é o produto”. (Ibidem)

[25] Os dados não são mais considerados estatísticos e obsoletos, cuja utilidade foi concluída uma vez que o objetivo para o qual foi coletado foi alcançado [...] Em vez disso, os dados tornaram-se uma matéria-prima dos negócios, um insumo econômico vital, usado para criar uma nova forma de valor econômico.

Deixa de ser curioso o fato de estar trocando mensagens sobre determinado assunto via WhatsApp, entrar no Face e se deparar com um anuncio que, coincidentemente, é sobre algo relacionado à conversa.

A inocência de achar que tudo se trata de uma mera coincidência incide diretamente na ignorância do usuário sobre o tratamento de seus dados pessoais, além dos vários obstáculos que são postos diante do mesmo, no intuito de dificultar a total compreensão da utilização destes dados.

Seguindo esse pensamento, se podemos definir o consumidor como um sujeito vulnerável, o usuário (titular dos dados pessoais) deve ser considerado como um sujeito hipervulnerável.

Podemos dizer que o cidadão é (hiper) vulnerável, já que em muitos casos não sabe sequer da coleta de seus dados pessoais, muito menos do poder para impedir tal coleta:

> [...] o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. (STJ, REsp 22.337-9/RS, 4ª Turma, Min. Rel. Ruy Rosado de Aguiar, julgado em 13.02.1995.)

Ainda:

> After investigating the subject of behavioral targeting intensively and extensively, our own ongoing uncertainty over what really is happening with information about our online activities suggests that notice, as yet, may not be sufficient for meaningful consent. Users who are subject to OBA confront not only significant hurdles but full-on barriers to achieving meaningful understanding of the practice and uses to which they are expected to be able to consent. This stems from various types of complexity and volatility in the ecology and dynamics of the industry, its policies, and its information flows.[26] (BARROCAS e NISSENBAUM, 2009, p. 05)

[26] Após investigar o tema da segmentação comportamental intensiva e extensivamente, nossa própria incerteza contínua sobre o que realmente está acontecendo com as informações sobre nossas atividades on-line sugere que o aviso, até o momento, pode não ser suficiente para um consentimento significativo. Os usuários que estão sujeitos à OBA enfrentam não apenas obstáculos significativos, mas barreiras completas para alcançar uma compreensão completada prática e dos usos com os quais se espera consentir. Isso decorre de vários tipos de complexidade e volatilidade na ecologia e dinâmica da indústria, suas políticas e seus fluxos de informação. (Tradução Nossa; Nota: OBA é sigla para Online Behavior Advertising, que é tradução para "publicidade comportamental online")

Ainda, quando o cidadão tem ciência da coleta de seus dados pessoais, este não tem noção de sua importância, e em muitos casos acaba “trocando” tais dados por vantagens irrisórias:

> O ser humano tem a tendência de focar nos benefícios imediatos, o que, de acordo com o arranjo e os modelos de negócios da economia informacional, é representado pelo acesso a um produto ou serviço on-line. Por tal razão, deixa de sopesar os possíveis prejuízos à privacidade, que são temporariamente distantes. De fato, os possíveis danos com relação à perda do controle sobre as informações pessoais só podem ser experimentados no futuro. (BIONI, 2019, p. 147).

Assim é evidente uma “[...] nova vulnerabilidade do consumidor em relação àqueles que detêm a informação pessoal.” (DONEDA, 2010, p. 09-10), ou seja, uma hipervulenerabilidade.

2.3.1 O *Big Data* e Os Meios De Mineração De Dados

Recentemente o termo “*Big Data*” se tornou muito popular, principalmente quando estamos falando de informações, mas poucos realmente sabem do que se trata.

Em um primeiro momento podemos conceituar “*Big Data”* como um grande resultado dos meios de coleta de dados, ou seja, uma grande massa de dados reunidos:

> [...] o conjunto de dados cuja existência só é possível em consequência da coleta massiva de dados que se tornou possível nos últimos anos, graças à onipresença de aparelhos e sensores na vida cotidiana e do número crescente de pessoas conectadas a tais tecnologias por meio de redes digitais e também de sensores. (ITS, 2016, p. 09)

Atualmente o “*Big Data*” pode ser usado para determinar as suas sugestões de amigos no “Facebook” ou sugestões de compras na “Amazon”, até mesmo aprimorar técnicas de negócios:

> Big data is used to determine your recommended friends on Facebook, suggested purchases on Amazon and the point at which your mobile phone

> network offers you a freebie to keep you on side. [27] (BURN-MURDOCH, 2012, s.p).

Ainda:

> […] because of big data, managers can measure, and hence know, radically more about their businesses, and directly translate that knowledge into improved decision making and performance.[28] (MCAFEE e BRYNJOLFSSON, 2012, s.p)

Contudo, a diferença entre o "Big Data" e outros meios de analisar dados, está em três elementos fundamentais: Volume, Velocidade e Variedade[29]:

> […] The big data movement, like analytics before it, seeks to glean intelligence from data and translate that into business advantage. However, there are three key differences: Volume […] Velocity […] Variety.[30] (MCAFEE e BRYNJOLFSSON, 2012, s.p)

O volume consiste na grande quantidade de dados que é possível coletar, como exemplo temos o Wallmart, que coletou cerca de "2,5 petabytes of data every hour from its costumers transactions" [31] (*Ibidem)*.

Devido à esse grande número de dados, e a grande agilidade no processamento, chegou-se ao ponto ser possível prever probabilidades de acontecimentos futuros:

> [...] tornando-se possível correlacionar uma série de fatos (dados), estabelecendo-se entre eles relações para desvendar padrões e, por conseguinte, inferir, inclusive, probabilidades de acontecimentos futuros. (BIONI, 2019, p. 41).

Foi graças a isso, que foi possível até mesmo prever onde um vírus poderia se espalhar, como é demonstrado pelos engenheiros do "Google" que

---

[27] Big data é usado para determinar suas recomendações de amigos no Facebook, sugestões de compras na Amazon e quando a sua operadora de telefone te oferecerá um brinde/promoção para te contudo, uma de suas grandes utilidades é a possibilidade de previsão manter no serviço.

[28] [...] por causa do Big Data, os gerentes podem medir e, portanto, conhecer radicalmente mais sobre seus negócios e traduzir diretamente esse conhecimento em decisões e desempenho aprimorados. (Tradução Nossa)

[29] Há aqueles que acrescentam outros dois elementos: "Big Data = volume + variedade + velocidade. Hoje adiciono mais dois "V"s: veracidade e valor" (IBM. Você realmente sabe o que é Big Data? 30 de abril de 2012. Disponível em: https://www.ibm.com/developerworks/community/blogs/ctaurion/entry/voce_realmente_sabe_o_que_e_big_data?lang=en. Acesso em: 04 de maio de 2019)

[30] O movimento do "Big Data", como métodos de análise anteriores, busca coletar inteligência dos dados e traduzi-los em vantagem comercial. No entanto, existem três diferenças fundamentais: Volume […] Velocidade […] Variedade (Tradução Nossa).

[31] 2,5 petabytes de dados toda hora das transações de seus clientes (Tradução Nossa)

utilizaram dados de pesquisas de seus usuários e traçaram uma previsão precisa de onde o vírus H1N1 poderia se espalhar, em 2009, nos Estados Unidos. Tais dados se mostraram mais eficazes do que os coletados pelo governo Norte Americano:

> As it happened, a few weeks before the H1N1 virus made headlines, engineers at the Internet giant Google published a remarkable paper in the scientific journal Nature. It created a splash among health officials and computer scientists but was otherwise overlooked. The authors explained how Google could “predict” the spread of the winter flu in the United States, not just nationally, but down to specific regions and even states. The company could achieve this by looking at what people were searching for on the Internet. Since Google receives more than three billion search queries every day and saves them all, it had plenty of data to work with [...] Thus when the H1N1 crisis struck in 2009, Google’s system proved to be a more useful and timely indicator than government statistics with their natural reporting lags.[32] (MAYER-SCHONEBERGER, Viktor; CUKIER, Kenneth, 2013, p. 01-02)

O segundo elemento que diferencia o “Big Data” é a velocidade, muitas vezes é necessário que se tenha uma informação em tempo real, atualmente qualquer pesquisa pode ser realizada em questão de segundos pelo “Google”, tal agilidade é fundamental principalmente se estamos tratando de previsões econômicas em uma bolsa de valores por exemplo.

Por fim a variedade consiste na ideia em que o “Big data takes the form of messages, updates, and images posted to social networks; readings from sensors;” [33] (MCAFEE e BRYNJOLFSSON, 2012, s.p).

Há vários outros meios de coletar ou minerar dados, como por exemplo os *cookies* (ou testemunhos de conexão[34]), que por vezes é utilizado pelos navegadores de *internet* e sites, principalmente para identificar ou rastrear dados uteis ou agilizar a navegação:

> Trata-se de programas de dados gerados com o objetivo principal de identificação do usuário, rastreamento e obtenção de dados úteis a seu

[32] Acontece que poucas semanas antes do vírus H1N1 ter sido manchete, engenheiros do gigante da internet Google publicaram um artigo notável na revista científica Nature. Isso criou um impacto entre as autoridades de saúde e os cientistas da computação, mas foi ignorado. Os autores explicaram como o Google poderia "prever" a disseminação da gripe de inverno nos Estados Unidos, não apenas nacionalmente, mas também em regiões específicas e até em estados. A empresa poderia conseguir isso observando o que as pessoas estavam procurando na Internet. Como o Google recebe mais de três bilhões de consultas de pesquisa todos os dias e salva todas, ele tinha muitos dados para trabalhar [...] Assim, quando a crise do H1N1 atingiu o país em 2009, o sistema do Google provou ser um indicador mais útil e oportuno do que as estatísticas do governo com suas defasagens naturais de relatórios. (Tradução nossa)

[33] Big Data toma forma pelas mensagens, atualizações, e imagens postadas nas redes sociais, leituras de sensores; [...] (Tradução Nossa).

[34] Termo utilizado pela GDPR em seu considerando 30

> respeito, especialmente, baseada em dados de navegação e de consumo. Tais fichários de dados, normalmente utilizados pelos provedores de Internet, são enviados aos navegadores dos usuários, em cujos computadores restam salvos em diretórios específicos. (MARTINS, 2008, p. 227-228).

Em um exemplo mais simples, o *cookie* é utilizado quando o usuário do "Facebook" acessa sua conta, logando-se automaticamente:

> [...] quando você entra com seu nome de usuário e senha em um site (como no Hotmail ou o orkut), o seu Firefox recebe e salva um ou mais cookies. Esses cookies servem como uma identificação que o Firefox envia em todos os acessos. Dessa forma o site pode reconhecer você como a pessoa que entrou anteriormente com o seu nome de usuário e senha. (COOKIES – O que são e como excluir.)

Dessa forma os *cookies* facilitam a navegação, já que em alguns casos permitem que o usuário entre em uma conta de determinado site, sem precisar fazer o "*login"*. Em troca dessa facilidade os sites e navegadores coletam dados pessoais de seus usuários:

> Para permitir carrinhos de compras, logins com validade duradoura e outros elementos que melhoram a experiência de navegação, os cookies pedem a privacidade do usuário em troca. Sites podem usar informações disponíveis nesses arquivos para compor um padrão de identificação na web, que não depende de visitas diretas ao site. Ao utilizar essa prática, uma loja pode conhecer seu padrão de consumo mesmo que você nunca tenha acessado o site da empresa antes. (ALVES, 2018, s.p)

Nessa situação percebe-se que muitos usuários optam utilizar cookies simplesmente para agilizar ou facilitar a sua navegação, trocando seus dados pessoais por isso.

É interessante destacar que os *cookies* podem ser apagados, trata-se de um processo semelhante ao de apagar o histórico de qualquer navegador, contudo, surgiram novas tecnologias que são "inapagáveis" e mais difíceis de serem bloqueadas, tratam-se dos *flash cookies* e HTML5 *web storages.*

No caso do *flash cookie*, trata-se de uma espécie de *cookie* relacionado ao programa *Adobe Flash Player,* tendo o potencial de rastrear páginas que são visitadas com mais frequência:

> Os flash cookies são geralmente utilizados pelo Adobe Flash Player e armazenam configurações relacionadas a vídeos e músicas, por exemplo. O maior problema dos flash cookies é que eles também podem armazenar identificadores, que são capazes de rastrear as páginas que você costuma

> visitar de uma forma mais frequente do que os cookies (PRIVACIDADE na internet: conheça os cookies, web beacons e flash cookies, 2013, s.p)

Não é possível apagar os *flash cookies* da mesma forma que se apaga os *cookies*, havendo um processo mais complexo para isso, contudo, alguns navegadores já possuem essa opção[35].

Enfim, o *Web Storage* é uma evolução dos *cookies*, suportando maiores quantidades de dados e possuem um método de armazenamento mais eficaz:

> With web storage, web applications can store data locally within the user's browser. Before HTML5, application data had to be stored in cookies, included in every server request. Web storage is more secure, and large amounts of data can be stored locally, without affecting website performance. Unlike cookies, the storage limit is far larger (at least 5MB) and information is never transferred to the server. [36](HTML5 Web Storage, sem data, s.p)

Assim, percebe-se que os cidadão é monitorado, em todos os seus passos na *internet*, pode-se dizer que tais dispositivos são as " [...] microtelas do século XXI que criam um estado de visibilidade constante do cidadão" (BIONI, 2019, p. 155), ressaltando a hipervulnerabilidade do cidadão em frente aos grandes "players" que gerenciam os seus dados pessoais.

2.4 Os Agentes De Tratamento De Dados e Os *Hackers* e *Crackers*

Será necessário para os nossos estudos futuros acerca da responsabilidade civil, analisarmos as figuras que atuam no tratamento de dados pessoais, desde os agentes que cumprem funções "legais" até aqueles que atuam ilicitamente com os dados.

A princípio há o operador, que seria "[...] pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;" (BRASIL, 2018, art. 5º, VII), ou seja, é a pessoa que atua diretamente

---

[35] Por exemplo o Google Chrome: https://www.tecmundo.com.br/google-chrome/9788-google-chrome-ganha-opcao-para-limpar-cookies-do-plugin-flash.htm

[36] Com o *Web Storage*, os aplicativos da Web podem armazenar dados localmente no navegador do usuário. Antes do HTML5, os dados de aplicativos precisavam ser armazenados em cookies, incluídos em todas as solicitações do servidor. O Web Storage é mais seguro e grandes quantidades de dados podem ser armazenadas localmente, sem afetar o desempenho do site. Ao contrário dos cookies, o limite de armazenamento é muito maior (pelo menos 5MB) e as informações nunca são transferidas para o servidor (Tradução Nossa).

com os dados pessoais, seguindo as formalidades legais e obedecendo as ordens do controlador.

Já o controlador por sua vez é “[...] pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;” (BRASIL, 2018, art. 5º, VI), dessa forma, esta figura não atua diretamente com os dados pessoais, sendo necessário o intermédio do operador, a quem dá ordens.

Para simplificar as definições, podemos entender o controlador como uma empresa, um banco por exemplo, que contrata outra para tratar dados relativos à sua atividade, esta última que seria o operador.

Nesse liame, há o encarregado, que seria:

> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). (Brasil, 2018, art. 5º, VIII)

O encarregado é equiparado à figura do *Data Protection Officer* constituído pela *General Data Protection Regulamentation* (art. 37).

Conforme demonstrado no tópico anterior, os *cookies*, *flash cookies* e o HTML5, podem ser usados para obter dados pessoais dos usuários, sendo bastantes utilizados por *crackers*. Consequentemente, torna-se necessário aprofundarmos os nossos estudos nestas figuras e nos crimes cibernéticos.

Em princípio é necessário distinguir o que é um *hacker* e o que é um *cracker*. O *hacker* pode ser definido como um *expert* na área da informática que modifica *softwares* e *hardwares,* contudo, utiliza sua *expertise* para desenvolver defesas contra invasores. Já o *cracker* tem um propósito oposto ao do *hacker*, utiliza sua *expertise* para invadir sistemas, com o intuito de tirar proveito de brechas:

> No submundo digital, a palavra hacker, no entanto, dificilmente é usada com sentido pejorativo. Ser considerado hacker é para a maioria dos aficionados por computadores um grande elogio. O termo que melhor designaria os invasores de sistemas seria cracker. Aliás, na grande maioria das páginas hackers a distinção é sempre deixada bem clara para os visitantes, com uma certa ingenuidade maniqueísta de que os hackers são os honrados senhores do espaço digital, ao passo que os crackers são aqueles hackers “maus” que se enveredaram pelas escusas trilhas da criminalidade cibernética. (VIANNA, 2001, p. 392).

Ainda:

> "Hacker" e "cracker" podem ser palavras parecidas, mas possuem significados bastante opostos no mundo da tecnologia. De uma forma geral, hackers são indivíduos que elaboram e modificam softwares e hardwares de computadores, seja desenvolvendo funcionalidades novas ou adaptando as antigas. Já cracker é o termo usado para designar quem pratica a quebra (ou cracking) de um sistema de segurança. (QUAL a diferente entre hacker e cracker?)

As atividades de *crackers* podem causar enormes prejuízos a empresas e aos usuários de determinado serviço. Temos como exemplo a invasão da rede online da Play Station, em que “[...] 100 milhões usuários no mundo tiveram dados como nome completo, endereço e número de cartão de crédito podem ter sido roubados.” (ENTENDA o ataque à rede on-line do PlayStation 3, a PSN, 2011).

Tais invasões podem inclusive comprometer grandes operações policiais, conforme visto recentemente pelas divulgações do site *The Intercept*, que anunciam várias supostas irregularidades no decorrer da operação Lava Jato[37].

No ordenamento brasileiro a invasão de um dispositivo informático tipifica do artigo 154-A do Código Penal, que foi incluído recentemente pela Lei Carolina Dieckmann.

Segundo tal dispositivo, incorre no crime aquele que:

> 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 [...]
> § 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*. (BRASIL, 1940, art. 154-A)

Há de se destacar que para outros crimes cometidos no meio cibernético é possível a aplicação de outros dispositivos do Código Penal, como é o caso da injúria no meio informático:

> No Código Penal, diversos tipos legais são pertinentes à criminalidade no mundo da informática. Para ofensas à honra alheia, tais como imputações de crimes, a calúnia (art. 138); na difusão de boatos humilhantes, a difamação (art. 139); e nos ataques pessoais, menosprezando as características da vítima, especialmente com apelidos grosseiros, a injúria (art. 140). Nas intimidações em geral, desponta o crime de ameaça (art. 147). Na invasão de conta bancária para desvio ou saque de valores, é de se reconhecer o furto

[37] Disponível em: https://theintercept.com/2019/06/29/chats-violacoes-moro-credibilidade-bolsonaro/

> (art. 155). Por sua vez, o envio de vírus para inutilizar equipamento ou seu conteúdo caracteriza o dano (art. 163). (MASSON, 2016, p. 330)

Em âmbito internacional, em 1986, a OECD reuniu um comitê de experts e criou uma pequena lista dos crimes cibernéticos:

> [...] An early start was made by the Organisation for Economic Co-operation and Developmente (OECD). In a 1986 report intitled Computer-Related Crime: Analysis of Legal Policy, the organisation recommended that members states pay particular attention to their coverage of specific knowingly committed acts under their national penal laws: 1. The input, alteration, erasure and/or suppression of computer data and/or computer programmes made willfully with the intent to commit an illegal transfer of funds or of another thing of value; 2. The input, alteration, erasure and/or suppression of computer data and/or computer programmes made willfully with the intent to commit a forgery; 3. The input, alteration, erasure and/or suppression of computer data and/or computer programmes, or other interference with computer systems, made willfully with the intent to hinder the functioning of a computer and/or telecommunication system; 4. The infringement of the exclusive right of the owner of a protected computer programme with the intent to exploit commercially the programme and put it on the Market; 5. The access to or the interception of a computer and/or telecommunication system made knowingly and without the authorisation of the person responsible for the system, either (i) by infringement of security measures or (ii) for other dishonest or harmful intentions. [38] (SMITH, Russell G.; GRABOSKY, Peter; URBAS, Gregor, 2004, p. 99)

Posteriormente, o Conselho Europeu, baseado na lista da OECD, criou uma segunda lista de crimes cibernéticos, dessa vez, abrangendo mais situações:

> [...] from this point, the Council of Europe moved on… another International Organisation, this founded in 1949 the Select Committee of Experts on Computer-Related Crime and the European Committee on Crime Problems prepared another List of Crimes: 1. Computer fraud; 2. Computer forgery; 3. Damage to computer data or computer programs; 4. Computer sabotage; 5. Unauthorized access; 6. Unauthorized interception; 7. Unauthorized

[38] Um começo precoce foi feito pela Organização para Cooperação Econômica e Desenvolvimento (OCDE). Em um relatório de 1986 intitulado Crime Relacionado ao Computador: Análise da Política Legal, a organização recomendou que os membros prestem atenção especial à sua cobertura de atos específicos conscientemente cometidos sob suas leis penais nacionais.1. A entrada, alteração, apagamento e / ou supressão de dados de computador e / ou programas de computador feitos intencionalmente com a intenção de cometer uma transferência ilegal de fundos ou de outra coisa de valor; 2. A entrada, alteração, apagamento e / ou supressão de dados de computador e / ou programas de computador feitos intencionalmente com a intenção de cometer uma falsificação; 3. A entrada, alteração, apagamento e / ou supressão de dados de computador e / ou programas de computador, ou outra interferência com sistemas de computador, feita voluntariamente com a intenção de impedir o funcionamento de um computador e / ou sistema de telecomunicações; 4. A violação do direito exclusivo do proprietário de um programa de computador protegido com a intenção de explorar comercialmente o programa e colocá-lo no mercado; 5. O acesso ou a intercepção de um sistema informático e / ou de telecomunicações feito conscientemente e sem a autorização da pessoa responsável pelo sistema, ou (i) por violação de medidas de segurança ou (ii) por outras intenções desonestas ou prejudiciais (Tradução Nossa).

> reproduction of a protected computer programme; 8. Unauthorized reproduction of a computer topography. [39] (MASSENO, sem data, p. 06)

Dessa forma, as grandes invasões são realizadas por *crackers* e não por *hackers* como grande parte dos noticiários demonstram, além disso, a *internet* não é um lugar desregrado como aparenta ser, vários dispositivos penais e civis podem ser aplicados mesmo em âmbito informático.

[39] [...] a partir deste ponto, o Conselho da Europa mudou-se para… outra Organização Internacional, fundada em 1949, o Comitê Seleto de Especialistas em Crime Relacionado a Computador e o Comitê Europeu sobre Problemas Criminosos prepararam outra Lista de Crimes: 1. Fraude de computador; 2. Falsificação de computadores; 3. Danos a dados de computador ou programas de computador; 4. Sabotagem por computador; 5. Acesso não autorizado; 6. Interceptação não autorizada; 7. Reprodução não autorizada de um programa de computador protegido; 8. Reprodução não autorizada de uma topografia de computador (Tradução Nossa).

3 PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL

No presente capítulo busca-se firmar a necessidade de tornar a proteção de dados pessoais em um direito fundamental. Para tanto, será necessário explicar o fenômeno da *datificação* e do *proffiling*, reforçando novamente a importância dos dados pessoais, além de trabalhar o tema da autodeterminação informacional. Claramente também será trabalhado o direito fundamental à privacidade, destacando a diferença entre tal direito e o direito à proteção de dados pessoais.

3.1 Biografia Digital: A Personificação Dos Dados

Um dos fenômenos mais importantes para a formação de uma biografia digital é a datificação, termo que foi empregado por Mayer-Schonenberger e Kenneth Cukier, em 2013, aplicado para definir a prática de registrar e reorganizar dados empregados pelo Comodoro Maury, e por Koshimizu:

> Today data refers to a description of something that allows it to be recorded, analyzed, and reorganized. There is no good term yet for the sorts of transformations produced by Commodore Maury and Professor Koshimizu. So let's call them datafication. To datafy a phenomenon is to put it in a quantified format so it can be tabulated and analyzed.[40] (MAYER-SCHONENBERGER, CUKIER, 2013, p. 74)

Os feitos do Comodoro Maury e de Koshimizu foram a transformações de informações reais em dados, que podem ser registrados e reorganizados, tornando assim a utilização destes mais simples.

O primeiro foi responsável por datificar dados importantes dos oceanos, o que tornou possível a instalação do primeiro cabo transatlântico:

> His work was essential for laying the first transatlantic cable. And, after a tragic collision on the hight seas, he quickly devised the system of shipping lanes that is commonplace today.[41] (MAYER-SCHONENBERGER, CUKIER, 2013, p. 76)

---

[40] Hoje, os dados referem-se a uma descrição de algo que pode ser registrado, analisado e reorganizado. Ainda não há um bom termo para os tipos de transformações produzidas pelo Comodoro Maury e por Koshimizu. Então, vamos chamá-los de datificação. Para documentar um fenômeno é colocá-lo em um formato quantificado para que possa ser tabulado e analisado (Tradução Nossa).

[41] Seu trabalho foi essencial para a instalação do primeiro cabo transatlântico. E, depois de uma colisão trágica nos mares altos, ele rapidamente inventou o sistema de rotas marítimas que é comum hoje em dia (Tradução Nossa).

Já o segundo foi responsável por extrair informações, baseando-se na maneira que uma pessoa se senta, dessa forma, organizando e tabulando tais dados:

> Few think that the way a person sits constitutes information, but it can. When a person is seated, the contour of the body, posture, and distribution of weight can all be quantified and tabulated. Koshimizu and his team of engineers convert backsides into data by measuring the pressure at 360 differents points from sensors in a car seat and indexing each point on a scale from zero to 256.[42] (MAYER-SCHONENBERGER, CUKIER, 2013, p. 77)

Contudo, é elementar distinguir a datificação da digitalização, este que é o ato de transportar uma informação análoga em números binários, ou seja, códigos que possibilitam a leitura por computadores. Já a datificação seria transformar informações reais em dados, que podem ser tabulados e reorganizados:

> Again, this is very different from digitization, the process of converting analog information into the zeros and ones of binary code so computers can handle it. Digization wasn't the first thing we did with computers. The initial era of the computer revolution was computational, as the etymology of the word suggests. [43] (MAYER-SCHONENBERGER, CUKIER, 2013, p. 78)

É possível datificar todo tipo de informação, inclusive emoções e relações pessoais, como é o exemplo do *Twitter*:

> Twitter enabled the datafication of sentiment by creating an easy way for people to record and share their stray thoughts, which had previously been lost to the winds of time. [44] (MAYER-SCHONENBERGER, CUKIER, 2013, p. 91)

Atualmente grande parte da população está *online*, poucos são aqueles que não estão conectados a uma rede social, seja no *Facebook*, *Twitter*, *LinkedIn* etc... visto isto, tais empresas começaram a se especializar no aspecto da

---

[42] Poucos pensam que a maneira como uma pessoa se senta constitui informação, mas pode. Quando uma pessoa está sentada, o contorno do corpo, postura e distribuição de peso podem ser quantificados e tabulados. Koshimizu e sua equipe de engenheiros converteram tais informações em dados medindo a pressão em 360 pontos diferentes dos sensores em um assento de carro e indexando cada ponto em uma escala de zero a 256 (Tradução Nossa).

[43] Novamente, isto é muito diferente da digitalização, o processo que converte informações analógicas em zeros e um's de código binário, para que os computadores possam lidar com isso. A digitalização não foi a primeira coisa que fizemos com computadores. A era inicial da revolução dos computadores foi computacional, como sugere a etimologia da palavra.

[44] O Twitter possibilitou a datificação do sentimento ao criar uma maneira fácil para as pessoas registrarem e compartilharem seus pensamentos dispersos, que antes eram perdidos para os ventos do tempo (Tradução Nossa).

comunicação *online*, encontrando meios de convencerem os usuários a transferirem suas interações sociais para o âmbito informático:

> À medida que as empresas de tecnologia começaram a se especializar em um ou vários aspectos da comunicação on-line, elas convenceram muitas pessoas a transferir parte de suas interações sociais para os ambientes da web. (DIJCK, 2017, p. 42)

Um dos meios de convencer os usuários a transferirem tais interações é a prestação de serviços *online*, conforme já visto, muitas vezes o cidadão troca seus dados pessoais por meras cortesias, na maioria das vezes por uma navegação mais prática ou para ter acesso a um determinado tipo de serviço.

Todos esses dados coletados são atrelados à *big data*, consequentemente, se reunirmos os dados do *Facebook, Twitter* e demais redes sociais será possível construir uma biografia digital da pessoa:

> In the Information Age, personal data is being combined to create a digital biography about us. Information that appears innocuous can sometimes be the missing link, the critical detail in one's digital biography, or the key necessary to unlock other stores of personal information. [45] (SOLOVE, 2004, p. 44).

E é nesse contexto que surge o termo *proffiling*, que seria o ato de formar um perfil de uma pessoa, tendo como base os seus dados pessoais: "É a prática conhecida como *profilling*, em que os dados pessoais de um indivíduo formam um perfil a seu respeito para a tomada de inúmeras decisões." (BIONI, 2019, p. 91). O *proffiling* é especialmente utilizado pelas propagandas direcionadas, nesse sentido, tais direcionamentos influenciam nas escolhas dos próprios titulares, o que afeta o desenvolvimento da personalidade desta pessoa.

Percebe-se que é possível dizer que parte da intimidade da pessoa, suas relações e até mesmo sua personalidade estão *online*, assim formando uma nova identidade da pessoa. Eventual uso inadequado dos dados pessoais pode ser uma agressão ao seu direito à privacidade e ao direito a proteção de dados pessoais.

---

[45] Na Era da Informação, os dados pessoais estão sendo combinados para criar uma biografia digital sobre nós. As informações que parecem inócuas podem, às vezes, ser o elo perdido, os detalhes críticos na biografia digital de uma pessoa ou a chave necessária para desbloquear outra gama de informações pessoais (Tradução nossa).

Pode-se sustentar que os dados pessoais estão relacionados aos direitos da personalidade, graças à esta biografia digital:

> Tendo em vista tratar-se de direito à personalidade, já que os dados armazenados representam a pessoa na sociedade, qualquer banco ou registro de dados pessoais deve ser entendido como público, independentemente de ser gerido por organismo privado ou estatal. [46] (MENDES, 2011, p. 19).

Tal raciocínio é reafirmado pela Lei Geral de Proteção de Dados Pessoais (Artigo 12 §2º), vez que estipula que os dados anonimizados (ou ainda que não pessoais), também podem ser utilizados para a formação de um *profilling* e impactarem a vida pessoal de um indivíduo, logo, podem ser considerados como dados pessoais:

> Daí a importância da alocação da proteção dos dados pessoais como um novo direito da personalidade. Com isso, permite-se um alcance normativo maior, que é capaz de abraçar toda e qualquer atividade de processamento de dados (ainda que não pessoais), mas que impacta a vida de um indivíduo. Essa é a racionalidade da LGPD ao prever que dados anonimizados podem ser considerados como dados pessoais caso sejam utilizados para formação de perfis comportamentais (art. 12 §2º). O foco está, portanto nas consequências que tal atividade de tratamento de dados pode ter sobre um sujeito (BIONI, 2019, p. 80)

Nesse contexto, há o simbólico julgamento do Tribunal Constitucional Alemão acerca da Lei do Censo de 1983, que inclui o direito a proteção de dados pessoais dentro dos direitos a personalidade e cria a autodeterminação informativa.

3.2 Autodeterminação Informativa

O termo “autodeterminação informativa” foi empregado primeiramente em um julgado simbólico da Corte Constitucional Alemã, que decidiu que a Lei do Censo de 1983 era em partes inconstitucional.

Tal lei objetivava coletar dados dos cidadãos alemães, contudo, era pouco especifica quanto ao proposito dessa coleta, além de haver sanções para aqueles que não cooperassem com a coleta de dados:

---

[46] Nesse sentido BIONI (2019, p. 64) e DONEDA (2016, p. 157).

> Esta lei previa que cada cidadão deveria responder a 160 perguntas, a serem posteriormente submetidas a tratamento informatizado. Alguns pontos da lei geraram controvérsias, entre eles: - a possiblidade de que os dados obtidos pelo censo fossem confrontados com os dados do registro civil para uma eventual retificação do próprio registro; - a possibilidade destes mesmos dados, desde que não identificados com o nome de cada titular, poderem ser transmitidos às autoridades federais e aos Länder; - a existência de uma multa pecuniária, relativamente elevada, para os que não respondessem, bem como um mecanismo de favorecimento àqueles que denunciassem tais pessoas (DONEDA, 2006, p. 193).

Ainda:

> O § 9 da Lei previa, entre outras, a possibilidade de uma comparação dos dados levantados com os registros públicos e também a transmissão de dados tornados anônimos a repartições públicas federais, estaduais e municipais para determinados fins de execução administrativa (MARTINS, 2005, p. 234).

Dessa forma, pouco se sabia quais eram os “determinados fins de execução administrativa”, e o fato de haver sanções para punir aqueles que não contribuíssem seria uma violação direta a “[...] alguns direitos fundamentais dos reclamantes, sobretudo o direito ao livre desenvolvimento da personalidade (Art. 2 I GG)” (MARTINS, 2005, p. 234).

Tais foram alguns dos motivos mais relevantes para o acionamento da corte alemã. Quanto aos motivos da decisão, estes contêm elementos essenciais para a projeção da proteção dos dados pessoais dentro dos direitos da personalidade.

O primeiro passo que a Corte Constitucional Alemã tomou foi tratar da importância dos dados pessoais, e o quanto são relevantes para a construção da personalidade de um indivíduo, isto é, já existia uma ideia da datificação e da biografia digital das pessoas, consequentemente, uma das bases centrais do julgado foi a aplicação das regras do direito da personalidade:

> O parâmetro do exame é em primeira linha o direito geral da personalidade protegido pelo Art. 2 I c. c. Art. 1 I GG [...] Quem não consegue determinar com suficiente segurança quais informações sobre sua pessoa são conhecidas em certas áreas de seu meio social, e quem não consegue avaliar mais ou menos o conhecimento de possíveis parceiros na comunicação, pode ser inibido substancialmente em sua liberdade de planejar ou decidir com autodeterminação. Daí resulta: O livre desenvolvimento da personalidade pressupõe, sob as modernas condições do processamento de dados, a proteção do indivíduo contra levantamento, armazenagem, uso e transmissão irrestritos de seus dados pessoais. Esta proteção, portanto, é abrangida pelo direito fundamental do Art. 2 I c. c. Art. 1 I GG. O direito fundamental garante o poder do cidadão de determinar em princípio ele mesmo sobre a exibição e o uso de seus dados pessoais (MARTINS, 2005, p. 236-238).

Surge assim, o termo autodeterminação funcional, que seria “[...] a liberdade de decisão sobre ações a serem procedidas ou omitidas e, inclusive, a possibilidade de se comportar realmente conforme tal decisão” (MARTINS, 2005, p. 237).

Para alguns autores seria “[...] o direito dos indivíduos de ‘decidirem por si próprios, quando e dentro de quais limites seus dados pessoais podem ser utilizados’” (DONEDA, 2006, p. 196 apud PANEBIANCO, 2000, p. 187, tradução do autor).

Contudo, segundo Bruno Bioni, deve-se entender a autodeterminação funcional, como algo a mais do que o simples consentimento do usuário:

> A relevância do julgado destaca-se por sua ratio decidendi sob dois aspectos: a) proteção dos dados pessoais como um direito de personalidade autônomo e a compreensão do termo autodeterminação informacional para além do consentimento [...] (BIONI, 2019, p. 101).

Em um primeiro momento, podemos interpretar a autodeterminação funcional como um direito incluído dentro dos direitos a personalidade, que além de requerer o consentimento do titular dos dados pessoais, impõe limites na utilização dos mesmos, tal limite que seria a finalidade para a qual se cedeu os dados, dando assim, maior controle ao cidadão sob os seus dados.

O julgado gerou várias consequências, entre elas a criação de uma nova lei que corrigiu a maioria dos pontos contestados, além de ter difundido a ideia da autodeterminação funcional:

> As consequências da sentença sobre o censo foram claras: uma nova lei, que veio a corrigir os pontos contestados, foi promulgada em 1985 para o censo que foi realizado em 1987. Neste novo censo, os dados coletados para fins estatísticos eram separados das informações individuadas; o cidadão era cuidadosamente informado sobre as finalidades da coleta de dados e sobre sua obrigação de fornecê-las; a transferência de dados entre autoridades federais e regionais foi simplesmente vetada, entre diversas outras disposições. (DONEDA, 2006, p. 196)

Além disso, o julgado é simbólico já que construiu um raciocínio de proteção de dados pessoais transpondo o público e privado, ou seja, não se limitando a dizer que o direito a proteção de dados pessoais estaria dentro do direito a privacidade:

> Portanto, o julgado é paradigmático na construção de um direito autônomo da personalidade relativo à proteção dos dados pessoais, o qual avança na compreensão de que a sua dinâmica se afasta da dicotomia entre público e privado (BIONI, 2019, p. 104)

O direito à autodeterminação informacional é debatido e desenvolvido até hoje, sendo elementar citar a importância do consentimento contextual para o instituto.

O consentimento é um ponto fundamental para a autodeterminação, porém, por si só, não seria o suficiente para a resolução de todos os conflitos, tendo em vista que o que deve ser considerado “não é somente se houve o consentimento dos titulares dos dados pessoais, mas se o fluxo informacional que lhes é subjacente é integro” (BIONI, 2019, p. 237).

Por isso o consentimento deve ser complementado pelo contexto, atribuindo-se assim à autodeterminação um novo elemento, o qual é denominado consentimento contextual ou privacidade contextual:

> Para limitar e se revelar como um relato normativo complementar à autodeterminação informacional centrada no consentimento, a privacidade contextual dela se aproxima ao propugnar que o controle dos dados pessoais deve ser visto sob as lentes das práticas sociais e não meramente individual [...] Ele não é delimitado por um proposito especifico e duro – em linha com o que dispõe a expressão finalidades determinadas -, mas direcionado a uma gama de ações passiveis de serem executadas no contexto de uma relação. Com isso, a privacidade contextual mostra-se útil, já que ela é elástica o suficiente para governar o uso secundário dos dados pessoais que não podem ser previamente especificados e controlados de maneira rígida (BIONI, 2019, p. 243).

Não quer dizer que somente a falta de consentimento seria uma violação à proteção de dados, mas também o emprego dos dados em um contexto fora do pressuposto. Nessa situação temos o caso da Smart TV’s da Samsung, que continha uma cláusula de uso que permitia a capitação de imagens e sons emitidos pelos usuários, não estipulando um momento exato dessa capitação, o que passa a impressão de que a empresa estaria espionando os consumidores e repassando os dados à terceiros[47].

O intuito da Smart TV é entretenimento, se a captação desses dados não estiver relacionada a esse objetivo, ou a este contexto, há uma clara violação a

[47] Recomenda-se a leitura: https://oglobo.globo.com/economia/apos-ser-acusada-de-espionar-os-consumidores-samsung-altera-politica-de-smart-tvs-15304244

autodeterminação informativa. Contudo, posteriormente, a empresa redigiu novamente a política de privacidade da TV:

> Se o Cliente ativar o Reconhecimento de Voz, poderá interagir com a Smart TV utilizando a respectiva voz. Para fornecer a funcionalidade Reconhecimento de Voz, os comandos de voz do Cliente serão transmitidos (juntamente com as informações sobre o dispositivo do Cliente, incluindo os identificadores do dispositivo) à Samsung e esta irá converter os comandos de voz do Cliente em texto para fornecer as funcionalidades de Reconhecimento de Voz. Para além disso, a Samsung poderá recolher os comandos de voz e os textos associados para que a Samsung possa avaliar e melhorar as funcionalidades. A Samsung recolherá apenas os comandos de voz do Cliente quando este fizer um pedido de pesquisa específico à Smart TV clicando no botão de ativação no comando ou no ecrã e falando ao microfone do comando. (POLÍTICA de privacidade da Samsung – suplemento da Smart TV, grifo nosso)

Na nova redação, a finalidade e o momento da captação dos dados são bem especificados, há o objetivo de melhorar as funcionalidades do aparato, consequentemente melhorar o entretenimento oferecido, portanto:

> A integridade do fluxo informacional está, diretamente, ligada com as funcionalidades por ele desempenhadas, a justificar as suas respectivas intrusões na vida dos seus usuários (BIONI, 2019, p. 237).

Assim, nesse contexto, a captação dos dados e a sua utilização são justificadas, o que torna o fluxo informacional integro.

Pode-se concluir que o direito à proteção de dados pessoais estão englobados nos direitos a personalidade (graças a formação de uma biografia digital e da datificação das coisas), garantindo ao cidadão maior controle dos seus dados, tendo em vista, a necessidade do consentimento e da utilização dos dados pessoais dentro de um contexto especifico, impondo limites na coleta de informações, além de garantir a veracidade das informações já coletadas.

3.3 Do Direito à Privacidade

Os primeiros debates acerca do direito à privacidade se iniciaram com o avanço tecnológico, em que informações privadas estavam sendo expostas de maneiras inimagináveis. Nesse sentido, o primeiro texto a debater o direito a privacidade foi o artigo norte-americano "*The Right of privacy*", que estabeleceu a primeira ideia de privacidade:

> The principle which protects personal writings and all other personal Productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality.[48] (WARREN; BRANDEIS, 1890, p. 205)

Tal pensamento surgiu justamente por conta dos avanços tecnológicos da época, buscando evitar que a privacidade das pessoas seja violada por meio de fotografias, ou outros meios de gravação:

> [...] a principle which may be invoked to protect the privacy of the individual from invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for recording or reproducing scenes or sounds. [49] (WARREN, BRANDEIS, 1890, p. 206)

Atualmente o direito à privacidade é consagrado no nosso ordenamento como um direito fundamental, concretizado por meio de uma clausula pétrea (art. 5º, X, Constituição Federal):

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; (BRASIL, 1988, art. 5º, X)

A constituição cita “intimidade” que pode ser definida como o espaço em que o indivíduo tem para se manter sozinho, afastando-se da sociedade e desenvolvendo ideias e pensamentos, que pretende manter fora do alcance popular:

> [...] a intimidade interior reveste-se de natureza física e material. O indivíduo afasta-se da multidão. Recolhe-se ao seu castelo. Desce às profundezas de sua alma e sai em busca de seu ser. (COSTA JR, 2007, p. 10-11)

O direito à privacidade tutela tal intimidade, podendo ser dividida em três esferas, a esfera da publicidade, que “[...] compreende os atos praticados em público

---

[48] O princípio que protege os textos pessoais e todas as outras produções pessoais, não contra roubo ou apropriação física, mas contra qualquer forma de publicação, é, na realidade, não o princípio da propriedade privada, mas da inviolabilidade (Tradução nossa).

[49] [...] um princípio que pode ser invocado para proteger a privacidade do indivíduo contra invasões, seja pela imprensa muito empreendedora, o fotógrafo ou o possuidor de qualquer outro dispositivo moderno para gravar ou reproduzir cenas ou sons (Tradução nossa).

com o desejo de torna-los públicos.” (NOVELINO, 2012, p. 504), a esfera pessoal, abrangendo “[...] as relações com o meio social sem que, no entanto, haja vontade ou interesse na divulgação [...]” (*ibidem*), e por fim a esfera íntima que se refere ao “[...] modo de ser de cada pessoa, ao mundo intrapsíquico aliado aos sentimentos identitários próprios (autoestima, autoconfiança) e à sexualidade” (*ibidem)*.

Nesse sentido, identifica-se duas esferas primordiais, a pública e a privada, e dentro desta última, encontra-se a intima, sendo que as esferas privada e intima são tutelados pelo direito à privacidade, restringindo o Estado à impor impedimentos (liberdade negativa):

> [...] o âmbito da privacidade plasmado no estatuto constitucional consiste, portanto, no conjunto de operações desenvolvidas por um indivíduo que restam imunes ao poder de ingerência estatal ou privada. (...) A privacidade envolve, assim, conceito fundamental do Estado Democrático de Direito ao redor do qual se estabelece uma relação jurídica cujo elemento básico é a imputação de um dever de abstenção e de sigilo, ou seja, de não intromissão e de não desvelamento de determinados aspectos pessoais do indivíduo. O resguardo da privacidade impõe, portanto, uma obrigação de não fazer, de silenciar (ZANON, 2012, p. 37)

Em suma, pode-se considerar o direito à privacidade como um direito a personalidade, que é dividido em três esferas (público, privado e íntimo), cujo o objetivo é resguardar as esferas privada e intima, assim, garantindo o livre desenvolvimento psicológico da pessoa.

3.4 Proteção de Dados Pessoais Como Um Direito Fundamental Autônomo à Privacidade

Grande parte dos direitos fundamentais consagrados pelo ordenamento jurídico brasileiro podem ser encontrados no artigo 5º da Constituição Federal, contudo, conforme o §2º do mesmo artigo, o rol de direitos não poderá excluir outros decorrentes de princípios ou de tratados internacionais.

Assim os direitos fundamentais, são normas abertas e indeterminadas, fundados em princípios, abrangendo várias situações, o que oferece proteção em diversas hipóteses, podendo assim ser conceituados como:

> [...] todas aquelas posições jurídicas concernentes às pessoas, que, do ponto de vista do direito constitucional positivo, foram, por seu conteúdo e importância (fundamentalidade em sentido material), integradas ao texto da

> Constituição e, portanto, retiradas da esfera de disponibilidade dos poderes constituídos (fundamentalidade formal), bem como as que, por seu conteúdo e significado, possam lhes ser equiparados, agregando-se à Constituição material, tendo, ou não, assento na Constituição formal (aqui considerada a abertura material do Catálogo). (SARLET, 2009, p. 77)

Tais direitos possuem quatro funções principais, sendo elas a de defesa ou liberdade, prestação social, proteção perante terceiros e a de não discriminação. Dentro da primeira, os direitos fundamentais visam proteger a pessoa humana e sua dignidade, contra atos do Estado:

> A primeira função dos direitos fundamentais – sobretudo dos direitos, liberdades e garantias – é a defesa da pessoa humana e da sua dignidade perante os poderes do Estado (e de outros esquemas políticos coercitivos). (CANOTILHO, 1993, 407).

A função de prestação social, exige que o Estado ofereça serviços de saúde, educação, segurança social e demais prestações: “Os direitos a prestação significam, em sentido estrito, direito do particular a obter através do Estado (saúde, educação, segurança social)” (CANOTILHO, 1993, 408).

Quanto a proteção perante terceiros, será obrigação estatal assegurar os direitos individuais, por meio de medidas coercitivas, contra eventuais agressões originadas de terceiros:

> Neste sentido o Estado tem o dever de proteger o direito à vida perante eventuais agressões de outros indivíduos (é a ideia trazida pela doutrina alemã na fórmula Schutzpflicht). O mesmo acontece com numerosos direitos como o direito de inviolabilidade de domicílio, o direito de protecção de dados informativos, o direito de associação. Em todos estes casos, de garantia constitucional de um direito resulta o dever do Estado adoptar medidas positivas destinadas a proteger o exercício dos direitos fundamentais perante atividades perturbadoras ou lesivas dos mesmos praticadas por terceiros. Daí o falar-se da função de proteção perante terceiros. (CANOTILHO, 1993, p. 409).

Por fim, a não discriminação, busca evitar que os cidadãos sejam tratados desigualmente, tal preceito é extraído diretamente do direito a isonomia:

> Uma das funções dos direitos fundamentais ultimamente mais acentuada pela doutrina (sobretudo a doutrina norte-americana) é a que se pode chamar de função de não discriminação. A partir do princípio de igualdade e dos direitos de igualdade específicos consagrados na constituição, a doutrina deriva esta função primária e básica dos direitos fundamentais: assegurar que o Estado trate os seus cidadãos como cidadãos fundamentalmente iguais. (CANOTILHO, 1993, p. 408, apud ORRÚ, 1998)

É nesse sentido que os direitos fundamentais atuam dentro do nosso ordenamento, na situação em que um destes for violado, a própria Constituição Federal disponibiliza vários meios para confrontar tal violação, entre estes podemos citar o *habeas data*.

Atualmente o *habeas data* é regulamentado pela lei 9.507 de 1997, também possui previsão constitucional (art. 5º, LXXII), sendo utilizado para três finalidades (art. 7º da lei 9.507):

> I - para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registro ou banco de dados de entidades governamentais ou de caráter público; II - para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo; III - para a anotação nos assentamentos do interessado, de contestação ou explicação sobre dado verdadeiro mas justificável e que esteja sob pendência judicial ou amigável. (BRASIL, 1997, art. 7º)

Percebe-se pela redação dos dispositivos que o *habeas data* faz, em partes, alusão ao direito a proteção de dados pessoais. Nesse sentido, alguns autores, interpretam o *habeas data* em conjunto com o direito à privacidade (art. 5º, X, Constituição Federal) chegando à um direito fundamental a proteção de dados pessoais:

> [...] quando se interpreta a norma do art. 5º, X, em conjunto com a garantia processual do *habeas data,* é possível extrair-se da Constituição Federal (LGL|1988\3) um verdadeiro direito fundamental à proteção de dados pessoais [...] à luz desse entendimento, verifica-se que a Constituição apresenta dois importantes mecanismos de tutela da personalidade contra o tratamento de dados: o direito material à proteção de dados pessoais, baseado no art. 5º, X, da CF/1998 (LGL\1988\3), e a garantia instrumental para a proteção desse direito, consubstanciada na ação do *habeas corpus* (art. 5º, LXXII, da CF/1988 (LGL\1998\3)). (MENDES, 2011, p. 14)

Ainda:

> [...] partindo do reconhecimento da proteção da informação pessoal pela ação de habeas data e do princípio fundamental da dignidade humana, é possível ampliar a garantia da inviolabilidade da intimidade e da vida privada para a proteção de dados pessoais. (MENDES, 2014, s.p)

Logo, segundo este entendimento, o direito fundamental a proteção de dados pessoais já estaria inserido implicitamente na Constituição Federal, como uma dimensão do direito à privacidade.

Pode ser percebido na diretiva 95/46/CE, que a proteção dos dados visa a proteção da privacidade:

> Artigo 1º
> Objecto da directiva
> 1. Os Estados-membros assegurarão, em conformidade com a presente directiva, a protecção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais. (EUROPA, 1995, s.p)

Contudo, a redação é diferente na *General Data Protection Regulation (GDPR)*:

> Art. 1 GDPR Subject-matter and objectives: […] 2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. [50] (EUROPA, 2016, s.p)

De outro lado, devido à natureza de direito atinente à personalidade que a proteção de dados possui, poderíamos engloba-lo dentro dos direitos fundamentais diante do fato da aproximação entre os direitos fundamentais e de personalidade:

> Muitos dos direitos fundamentais são direitos de personalidade mas nem todos os direitos fundamentais são direitos de personalidade. Os direitos de personalidade abarcam certamente os direitos de estado (por ex.: direito de cidadania), os direitos sobre a própria pessoa (direito à vida, à integridade moral e física, direito à privacidade), os direitos distintivos da personalidade (liberdade de expressão). Tradicionalmente, afastavam-se dos direitos de personalidade os direitos fundamentais políticos e os direitos a prestação por não serem atinentes ao ser como pessoa. Contudo, hoje em dia, dada a interdependência entre o estatuto positivo e o estatuto negativo do cidadão, e em face da concepção de um direito geral de personalidade como << direito à pessoa ser e à pessoa devir>>, cada vez mais os direitos fundamentais tendem a ser direitos de personalidade e vice-versa. (CANOTILHO, 2002, p. 396, apud, CARVALHO, 1970, p. 36).

Em relação a outros Estados, pequena parte destes já positivaram explicitamente o direito a proteção de dados pessoais em suas respectivas Cartas Magnas, como por exemplo Portugal:

> Artigo 35. (Utilização da informática)
> 1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.

[50] Art. 1 GDPR Matéria Subjetiva e objetivos: [...] 2. Esta regulamentação protege os direitos fundamentais e liberdades da pessoa natural em particular o direito à proteção de dados pessoais (Tradução Nossa).

> 2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente.
> 3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.
> 4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei.
> 5. É proibida a atribuição de um número nacional único aos cidadãos.
> 6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de protecção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.
> 7. Os dados pessoais constantes de ficheiros manuais gozam de protecção idêntica à prevista nos números anteriores, nos termos da lei. (PORTUGAL, 1976, art. 35)

Um dos fundamentos da positivação constitucional do direito na Constituição portuguesa é a relação que os dados pessoais têm com o princípio da dignidade da pessoa humana e ao desenvolvimento de sua personalidade, tornando assim, imprescindível a tutela constitucional:

> O Conjunto de direitos fundamentais relacionados com o tratamento informático de dados pessoais (cfr. Anotação IV, infra) arranca de alguns <<direitos-mãe>> em sede de direitos, liberdades e garantias. É o caso do direito à dignidade da pessoa humana, do desenvolvimento da personalidade, da integridade pessoal e da autodeterminação informativa. O enunciado <<dados pessoais>> exprime logo a estreita conexão entre estes direitos e o respectivo tratamento informático; podendo afirmar-se que quanto mais os dados relacionam a dignidade, a personalidade e a autodeterminação das pessoas, tanto mais se impõem restrições quanto à sua utilização e escolha (banco de dados). (CANOTILHO, 2007, p. 551)

Ressalta-se que na interpretação de Canotilho, os dados pessoais estariam ligados à dignidade da pessoa humana, integridade pessoal e autodeterminação informativa, contudo, não cita a privacidade.

Diferente da Constituição Portuguesa, a Espanhola utilizou como base o direito à privacidade ao tratar dos dados pessoais:

> Artículo 18. – [...] 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos[...] Art. 105. – [...] b) La Ley regulará el acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte

> a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas.[51] (ESPANHA, 1978, art. 18)

Já na América Latina, o Chile, em 2018, por meio da lei nº 2.109, é o exemplo mais recente:

> Artículo 19. - La Constitución asegura a todas las personas: [...] 4º.- El respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley;[52] (CHILE, 2005, art. 19)

Percebe-se que o direito a proteção de dados pessoais está caminhando para se tornar um direito fundamental, sendo como uma dimensão do direito à privacidade ou até mesmo como um direito autônomo.

3.4.1 Dicotomia Entre o Público e Privado: A Diferença Entre Direito à Privacidade e Proteção de Dados Pessoais

Como visto, os dados pessoais na atualidade tornaram-se o "petróleo" desta nova revolução, sendo um "recurso" estratégico para a tomada de decisões, principalmente devido ao fato de que tais dados formarem uma biografia digital dos seus titulares, que muitas vezes estão (hiper) vulneráveis em frente aos grandes *players*.

Dessa maneira, por ser um direito ligado a personalidade da pessoa deve ter amparo como um direito fundamental, havendo aqueles que dissertam que a proteção de dados pessoais seria uma dimensão do direito à privacidade:

> (c) o direito fundamental à intimidade e à vida privada, previsto no art. 5.º, X, da CF/1988 (LGL\1988\3), protege a esfera privada do indivíduo em diversas dimensões, inclusive na dimensão da privacidade dos seus dados pessoais e da autodeterminação de suas informações; (MENDES, 2011, p. 23).

---

[51] Art. 18 [...] 4. A lei limitará o uso da informática para garantir a honra e a intimidade pessoal e familiar dos cidadãos e o pleno exercício dos seus direitos. [...] Art. 105: [...] b) O acesso dos cidadãos aos arquivos e registos administrativos, salvo no que afete à segurança e defesa do Estado, a averiguação dos delitos e a intimidade das pessoas (Tradução Nossa).

[52] Articulo 19. – A Constituição assegura a todas as pessoas: [...] O respeito e a proteção a vida privada e a honra da pessoa e sua família, e também, a proteção de seus dados pessoais. O tratamento e proteção destes dados se efetuará na forma e condições que determinar a lei.

Esse é um raciocínio baseado na ideia de que os dados pessoais estão inseridos dentro da esfera da intimidade do titular, logo, estando sob o âmbito do direito à privacidade, sendo englobado dentro da proteção constitucional. Sustenta-se tal tese baseando-se na aplicação de *habeas data* para a tutela de dados pessoais.

Porém, com a máxima *vênia,* pensar neste direito como uma evolução do direito à privacidade é limitar o campo de proteção daquele:

> Ao derivarmos a proteção de dados pessoais diretamente da privacidade, tal qual espécie e subespécie, existe uma extensão da tutela da privacidade à proteção de dados pessoais. Tal operação, se basta para abarcar a disciplina sob a égide constitucional, arrisca porém simplificar os fundamentos da tutela dos dados pessoais a eventualmente limitar o seu alcance (DONEDA, 2006, p.326)

Ainda:

> O direito à proteção de dados não se limita à proteção da personalidade humana, sua intimidade e vida privada. A proteção de dados visa permitir gama muito maior de relações, ou, de outra parte, evitar que se criem barreiras para a fruição de todos os direitos e garantias. É fonte de fomento para igualdade social. (ROTUNDO, 2017, p. 10)

Em suma, devemos pensar na proteção de dados pessoais como um direito a personalidade derivado "[...] da tutela da privacidade porém não limitada por esta, e que faz referência a um leque de garantias fundamentais que se encontram no ordenamento brasileiro" (DONEDA, 2006, p. 326).

Nesse sentido, relembrando o julgado da lei do censo de 1983 da Alemanha, a Corte Constitucional Alemã cria a autodeterminação informacional fundamentada como um direito a personalidade, utilizando-se os preceitos básicos destes direitos, e não como uma dimensão da privacidade.

O direito à privacidade foca sua tutela no âmbito privado e da intimidade da pessoa, enquanto o direito a proteção de dados pessoais estaria focado em ambas as esferas, a privada e a pública, nesse último a discussão paira na veracidade dos dados pessoais públicos:

> Seria contraproducente e até mesmo incoerente pensar a proteção de dados pessoais somente sob as lentes do direito à privacidade. O eixo da privacidade está ligado ao controle de informações pessoais do que seja algo íntimo ou privado do sujeito. A proteção dos dados pessoas não se satisfaz com tal técnica normativa, uma vez que a informação pode estar sob a esfera

> pública, discutindo-se, apenas, a sua exatidão, por exemplo. (BIONI, 2019, p. 67).

Qualquer tipo de cadastro de banco de dados pessoais, mesmo que não envolvam a vida privada da pessoa, será amparado pelo direito a proteção de dados pessoais, o que não ocorreria na esfera do direito à privacidade, dessa forma, abrangendo mais liberdades individuais que as abarcadas pela privacidade:

> Significa dizer que mesmo os cadastros e bancos de dados formados com dados pessoais que não envolvam aspectos da intimidade e vida privada do indivíduo submetem-se às regras do direito à proteção de dados pessoais. Essa concepção depende, sobretudo, da percepção de que até as informações aparentemente mais inócuas podem ser integradas a outras e provocar danos ao seu titular (ZANON, 2012, p. 147)

Outra diferença fundamental, está nos bens jurídicos tutelados, o direito à privacidade tutela a necessidade do ser humano de ter um espaço privado e íntimo, o que influencia diretamente na psique do indivíduo, já a proteção dos dados, visa evitar que o titular seja “rotulado” pelos seus dados pessoais:

> Os bens jurídicos tutelados pela privacidade e pelo direito à proteção dos dados pessoais não são coincidentes. Na privacidade tutela-se a integridade psíquica do indivíduo (a necessidade humana de ter para sim uma esfera de reserva). A proteção dos dados pessoais resguarda a pessoa de não ser discriminada pelas suas crenças religiosas, suas opiniões políticas e filosóficas, por sua etnia, condições de saúde ou orientação sexual; proteger os dados pessoais significa também evitar que o indivíduo seja impedido de acessar bens e serviços, a princípio só oferecidos àqueles com ‘bons credenciais’; conferir proteção aos dados pessoais implica, ainda, livrar-se de etiquetas e chancelas (ZANON, 2012, p. 178-179).

Evitando eventuais práticas discriminatórias:

> Além disso, observa-se que cada vez mais a atividade de tratamento de dados impacta a vida das pessoas, em particular quando elas são submetidas a processos de decisões automatizadas que irão definir seu próprio futuro. Nesse contexto, o direito à proteção de dados pessoais tutela a própria dimensão relacional da pessoa humana, em especial para que tais decisões não ocasionem práticas discriminatórias, o que extrapola e muito o âmbito da tutela do direito à privacidade. (BIONI, 2019, p. 99)

É interessante salientar que para Zanon, a proteção de dados também visa beneficiar aqueles que possuem boas credenciais, ou seja, em âmbito dos bancos de dados positivos.

Percebe-se que a proteção de dados pessoais cumpre com as funções estabelecidas por Canotilho acerca dos direitos fundamentais, sendo uma proteção contra o tratamento inadequado dos dados pessoais pelo Estado (afinal a autodeterminação informacional surgiu com um questionamento da lei do censo de 1893 da Alemanha) e terceiros, além de evitar a “etiquetação” ou discriminação dos titulares. Claramente agora com a Lei Geral de Proteção de Dados Pessoais, e outros dispositivos em leis esparsas (Marco Civil da Internet e Código de Defesa do Consumidor), o Estado oferece uma proteção maior aos dados pessoais.

Daí vem a necessidade de desagregar o direito a proteção de dados pessoais do direito à privacidade, nesse sentido o Senado Federal, propôs um Projeto de Emenda Constitucional (PEC nº 17 de 2019[53]), cujo objeto é dispor a proteção de dados como um direito fundamental autônomo:

> De fato, a privacidade tem sido o ponto de partida de discussões e regulações dessa natureza, mas já se vislumbra, dadas as suas peculiaridades, uma autonomia valorativa em torno da proteção de dados pessoais, de maneira, inclusive, a merecer tornar-se um direito constitucionalmente assegurado. (BRASIL, 2019, p. 03)

Há aqueles que criticam a PEC por ser prematura, vez que a Lei Geral de Proteção de Dados Pessoais ainda não está vigente, e não há debate desenvolvido acerca do tema. Não é um pensamento equivocado, já que grande parte do debate brasileiro desenvolvido acerca dos dados pessoais utilizava como base o direito à privacidade.

É certo que a proteção de dados pessoais deve ser concretizada como um direito fundamental autônomo, por todos os motivos já expostos, entretanto, será necessário desenvolver melhor o direito autonomamente, principalmente nos tribunais, além da necessidade de estudarmos as consequências no ordenamento jurídico brasileiro.

[53] Atualmente a PEC tramita na Câmara dos Deputados (07 de agosto de 2019).

4. RESPONSABILIDADE CIVIL NA LGPD

Este capitulo tem a finalidade exclusiva de desenvolver os dispositivos da lei nº 13.709, a Lei Geral de Proteção de Dados Pessoais, desenvolvendo um entendimento acerca da responsabilidade tratada pela mesma. Para tanto, todos os conceitos trabalhados até o momento serão de grande importância, além disso, será necessário analisarmos a lei, desde o contexto mundial na época da sua criação, os seus limites e princípios, para enfim, dissertarmos acerca da responsabilidade civil na LGPD.

4.1 Breve Contexto Histórico Da Criação Da Lei

Em 2016 os Estados Unidos passavam por mais um período de eleições, dois eram os grandes candidatos, Donald Trump e Hilary Clinton. Contudo, tais eleições não foram só gravadas pela disputa entre o republicano e a democrata, mas sim pelo grande vazamento de dados pessoais que pode ter influenciado as eleições, e o Facebook tem grande importância nesse acontecimento.

O Facebook atualmente é uma das maiores redes sociais, e de fato, trabalha com uma grande quantidade de usuários, consequentemente com bilhões de dados.

Sabe-se que grande parte das relações pessoais estão datificadas no site, o que faz da rede social um grande conjunto de biografias digitais, assim, informações coletadas ou publicadas por grandes influenciadores, podem gerar grandes impactos na sociedade.

Nessa situação, poucos usuários têm noção do potencial dos seus dados armazenados pelo Facebook, e muitas vezes, os sedem por quaisquer bagatelas, é o caso dos famosos “*quizes*” que podem ser facilmente encontrados na plataforma.

Já é muito comum “deslizar” pela linha do tempo do Facebook e encontrar um compartilhamento de um amigo divulgando o seu resultado em um destes testes.

Há pouco tempo, por exemplo, o aplicativo FaceApp fazia muito sucesso no Brasil, com o intuito meramente de diversão, o *software* utilizava uma foto do

usuário para mostrar uma suposta versão envelhecida do mesmo, contudo, poucos sabem ao menos qual empresa que criou o aplicativo[54].

O Facebook permite que estes aplicativos tenham acesso aos perfis de seus usuários, em alguns casos para fins de pesquisas, ou meramente entretenimento.

Seria o caso do teste criado por Aleksander Kogan, da Universidade de Cambridge, Reino Unido, que criou o mesmo, com o preceito de fazer estudos psicológicos dos usuários da rede social.

Cerca de duzentas e setenta mil pessoas fizeram o teste, contudo, o sistema criado coletava os dados dos amigos destas pessoas, assim, cerca de cinquenta milhões de pessoas tiveram seus dados coletados diretamente ou indiretamente. Posteriormente, Kogan repassou as informações para a Cambridge Analytica, que revelou o esquema ao jornal The Guardian:

> Mesmo que só 270 mil pessoas tenham feito o teste de Kogan, o sistema permitiu que sua equipe visse o perfil de 50 milhões de usuários, pois também captava as informações de todos os amigos delas. No ano seguinte, Kogan repassou essa informação à Cambridge Analytica, que então contratou outros especialistas, entre eles Christopher Wylie, que acabou revelando o esquema ao jornal britânico The Observer (a versão dominical do Guardian) para influenciar a eleição dos EUA. (MARTÍ, 2018, s.p)

Há aqueles que dizem que a empresa britânica comprou os dados, com o objetivo de influenciar nas eleições, vez que a Cambridge Analytica, à época dos acontecimentos, era presidida por um dos assessores de Trump:

> A empresa é propriedade do bilionário do mercado financeiro Robert Mercer e era presidida, à época, por Steve Bannon, então principal assessor de Trump. A Cambridge Analytica teria comprado acesso a informações pessoais de usuários do Facebook e usado esses dados para criar um sistema que permitiu predizer e influenciar as escolhas dos eleitores nas urnas, segundo a investigação dos jornais The Guardian e The New York Times. (ENTENDA o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades, 2018, s.p)

Existem outros casos que influenciaram a criação da lei, como a suposta venda de dados pessoais pela SERPRO, em que segundo as investigações os:

---

[54] Recomenda-se a leitura: https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2019/07/17/febre-de-aplicativo-que-envelhece-rostos-faz-usuarios-ignorarem-riscos.ghtml

> [...] dados como endereço, nome da mãe, sexo e data de nascimento de inscritos no Cadastro de Pessoas Físicas (CPF) e Jurídica (CNPJ, estavam sendo comercializados por até R$273 mil. (MARQUES, 2018, s.p)

A repercussão destes casos foi tanta que em 04 de junho de 2018, a Câmara dos Deputados propôs o Projeto de Lei nº 53 de 2018, que culminou na Lei Geral de Proteção de Dados Pessoais.

4.2 Alcance Territorial e Material Da Lei

A princípio, a Lei Geral de Proteção de Dados Pessoais em seus dispositivos gerais estabelece seus limites territoriais, tratando-se de um tema que possui certa relevância, vez que grande parte das empresas que controlam os dados pessoais se encontram em território estrangeiro.

Nesse sentido, o artigo 3º da lei 13.709/2018 estipula que o tratamento realizado por pessoa física ou jurídica, estrangeiro ou nacional, com sede no Brasil ou fora, público ou privado, pouco importando o país em que os dados estão sendo tratados, serão abrangidos pela lei*:*

> Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
> I - a operação de tratamento seja realizada no território nacional;
> II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (Redação dada pela Lei nº 13.853, de 2019)
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
> § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.
> § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei. (BRASIL, 2018, art. 3)

Há certas hipóteses (alternativas) em que será aplicada a lei brasileira, a primeira quando o tratamento dos dados for realizado no território nacional, assim, diante de uma interpretação literal do dispositivo, pouco importa se os dados são coletados fora do país.

Já o inciso II apresenta duas situações, quanto ao objetivo do tratamento (oferta de bens ou o fornecimento de serviços) e à localidade do titular do dado

pessoal. Em relação ao objetivo, a lei segue a ideia do Marco Civil da Internet, em seu art. 11, § 2º [55]:

> 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.
> [...] § 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. (BRASIL, 2018, art. 11, Grifo Nosso)

A segunda parte do inciso cita o tratamento de dados de indivíduos localizados no território nacional, novamente utilizando-se de uma interpretação literal, pode-se dizer que não importaria se o dado pessoal foi coletado fora do país, ou até mesmo se o tratamento está sendo realizado em outro local, desde que o indivíduo esteja dentro do território brasileiro seus dados já são protegidos pela LGPD.

O inciso III trabalha a hipótese em que o dado é coletado em território nacional, que é complementado pelo §1º, ou seja, será considerado dado pessoal coletado em âmbito nacional os dados cujo titular nele se encontre no momento da coleta.

Em relação aos limites materiais da lei, será necessário relembrarmos o conceito de dados pessoais. Segundo o artigo 5º da Lei Geral de Proteção de Dados Pessoais, que adota a teoria expansionista, os dados pessoais seriam: “I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;”.

Logo, todo dado que identificar ou possibilitar a identificação do seu titular poderá ser considerado um dado pessoal, todavia, atualmente a maioria (se não todos) dos dados da internet podem se enquadrar no termo “identificável”, vez que pelos métodos de desanonimização é possível identificar os seus titulares.

Ao definir dados pessoais devemos nos atentar ao artigo 12 da LGPD, tal dispositivo visa limitar o conceito de dados pessoais. O artigo cita que os dados anônimos não serão considerados dados pessoais, a não ser que sejam convertidos por meios razoáveis (art. 12, *caput*):

---

[55] Nesse sentido: PINHEIRO (2018, p. 55)

> Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. (BRASIL, 2018, art. 12, Grifo nosso)

Os meios razoáveis dos quais o *caput* se refere, são aqueles que levam em consideração os custos e o tempo necessários para reverter o processo de anonimização (art. 12 §1º):

> § 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios. (BRASIL, 2018, art. 12, §1º, Grifo nosso)

Conforme já citado, os critérios adotados para definir dados pessoais tem grande importância, pois sem um limitador, todos os dados anônimos poderiam ser considerados como dados pessoais, o que acarretaria em uma redundância normativa.

Outro ponto fundamental do artigo 12 é o seu §2º, que cita:

> § 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada. (BRASIL, 2018, art. 12, §2º)

Tal parágrafo reafirma a proteção de dados pessoais dentro dos direitos a personalidade, já que se dá uma ênfase maior aos dados anônimos utilizados para a formação de perfis comportamentais ou *proffiling*:

> Daí a importância da alocação da proteção dos dados pessoais como um direito da personalidade [...] Essa é a da LGPD ao prever que dados anonimizados podem ser considerados como dados pessoais caso sejam utilizados para a formação de perfis comportamentais (art. 12, §2º). (BIONI, 2019, p. 80)

Se interpretarmos o §2º de maneira literal, percebe-se que estaríamos diante de um dispositivo “morto”, já que se o titular dos dados anônimos for identificado (por meios razoáveis), estaríamos diante da situação descrita pelo artigo 12, *caput*, e §1º.

Assim é necessário interpretar o parágrafo sistematicamente, baseando-se nos preceitos estabelecidos pela própria lei (art. 2º) e no conceito de

dados pessoais. Sabe-se que dispositivo visa proteger o livre desenvolvimento da personalidade do titular dos dados, tendo em vista que o *profilling* tem efeito direto no comportamento das pessoas, dessa forma, o parágrafo visa expandir a proteção legal para os dados anônimos que são utilizados para esta função, mesmo que não individualizados:

> Essa é uma interpretação sistemática do artigo que está em linha com o próprio conceito expansionista de dados pessoais – pessoa identificável e não somente identificada –, bem como um dos objetivos e fundamentos da própria lei – o livre desenvolvimento da personalidade (arts. 1º e 2º, VII). Não faria sentido, também sob o prisma de uma interpretação teleológica, prever uma exceção pela qual dados anonimizados estariam dentro do escopo da lei, mas que dela não seria possível alcançar situações nas quais um grupo de indivíduos (pessoas identificáveis) tem as suas respectivas liberdades (desenvolvimento da personalidade e direitos fundamentais) afetadas pelo uso de tais dados. Garante-se, com isso, uma *exegese* que torna o §2º do art. 12 aplicável e "não letra morta". E, sobretudo, coerente com o conceito de dado pessoal que foi desenhado e é vocacionado para expandir a proteção da pessoa natural com relação às situações nas quais a atividade de tratamento de dados – mesmo que anonimizados – afeta o livre desenvolvimento da sua personalidade. (BIONI, 2019, p. 81, Grifo nosso)

É um entendimento que pode ser fundamentado também nos debates no Congresso Nacional:

> Em vez da expressão "se identificada", constava a locução "ainda que não identificada" no então PLPDP/EXE. Essa investigação histórica do processo legislativo reforça uma interpretação teleológica no sentido de que o parágrafo em questão foi projetado para expandir a proteção da pessoa natural, ainda que o perfil comportamental não a individualize diretamente. (BIONI, 2019, p. 81)

Em relação ao §3º, é estabelecido que a autoridade nacional irá dispor sobre os métodos de anonimização citados pelo *caput* e §2º do artigo 12.

Devemos considerar que alguns dados pessoais não são abarcados pela proteção legal, trata-se do rol descrito pelo art. 4º, que se fundamenta na liberdade de imprensa e livre manifestação cultural e artística, preservação do Estado Democrático de Direito, ou o simples uso dos dados para fins particulares e não econômicos.

Assim, pode-se concluir que a Lei Geral de Proteção de Dados Pessoais, abrange os dados que já identificam os seus titulares, ou tem potencial para isso (identificável) – com exceção dos citados pelo rol do art. 4º. Em relação aos dados anônimos devemos pondera-los por meio da razoabilidade para serem abarcados pela

proteção legal, além disso, é preciso considerar aqueles que são utilizados para formação de perfis comportamentais.

4.3 Princípios Da Proteção de Dados

A Lei Geral de Proteção de Dados Pessoais traz em seu rol do artigo 6º uma série de princípios, dentre os quais, a maioria será trabalhada neste sub tópico, porém será dado maior ênfase aos princípios ligados à eventuais obrigações do controlador e do operador.

Os três primeiros princípios vinculados no artigo (finalidade, adequação e necessidade) são princípios "[...] que somados resultam no que se chama de mínimo essencial" (TEIXEIRA, ARMELIN, 2019, p. 47).

Pode-se entender que todo tratamento de dados pessoais que estiver de acordo com estes três princípios dificilmente incorrerá em violações legais previstos na Lei Geral de Proteção de Dados Pessoais:

> Desde modo, que a coleta, armazenamento, tratamento, compartilhamento e qualquer uso de dados pessoais seja sempre realizado com base nos princípios da finalidade, adequação e necessidade, de forma que em assim sendo será muito difícil que ocorra uma violação legal de algum direito previsto na Lei Geral de Proteção de Dados Pessoais. (LOPES; TEIXEIRA; TAKADA; 2019, p. 279)

O princípio da finalidade vincula todo tratamento de dados pessoais à uma finalidade especifica que justifique a sua coleta, sendo uma das bases para o consentimento contextual:

> [...] princípio da finalidade, que vincula o tratamento de dados pessoais à finalidade que motivou e justificou a sua coleta. A aplicação desse poderoso princípio tem como consequência a concretização de algumas das finalidades últimas da Lei, qual seja a consideração de que o tratamento de dados pessoais são indissociáveis de uma determinada função que sempre poderá ser avaliada, ou mesmo que dados pessoais, por estarem de certa forma "afetados" por uma finalidade, jamais poderão ser considerados como mera res in commercium. (MENDES, 2018, p. 04)

Encontra-se o princípio da finalidade da coleta de dados pessoais na Lei do Cadastro Positivo[56] e no Marco Civil da Internet[57] estando também "[...] implícito no Código de Defesa do Consumidor (Lei n. 8087/1990)" (TEIXEIRA; ARMELIN, 2019, p. 46).

Segundo a Lei Geral de Proteção de Dados Pessoais futura incompatibilidade com tal finalidade impossibilitará o tratamento de dados (art. 6º, I, Lei nº 13.709/18):

> 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; (BRASIL, 2018, art. 6º, Grifo Nosso).

A adequação está ligada diretamente com o consentimento contextual, visando regular o correto fluxo informacional dos dados pessoais, ou seja, busca-se por este princípio "[...] a compatibilidade do tratamento com as finalidades informadas ao titular" (BRASIL, 2018, Art. 6º), quanto a necessidade seria a "[...] limitação do tratamento ao mínimo necessário para a realização de suas finalidades" (BRASIL, 2018, Art. 6º), assim:

> [...] depois de haver sido comunicado ao titular de dados para que seus dados estão sendo coletados, a utilização dos mesmos deve ser fiel ao que foi uma vez informado, e não apenas isso, mas também de forma restrita, de maneira que os dados só sejam usados dentro da estrita necessidade. (LOPES; TEIXEIRA; TAKADA; 2019, p. 278-279)

O princípio do livre acesso basicamente garante aos titulares dos dados a consulta livre e gratuita de informações como: a duração, forma do tratamento, e a integralidade dos dados.

Tal princípio é trabalhado pelo artigo 9º da lei 13.709/18, que impõe o livre acesso à finalidade especifica do tratamento, duração, identificação do controlador, compartilhamento de dados pelo controlador e outros:

---

[56] Art. 5º São direitos do cadastrado: VII - ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados.

[57] Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: 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;

> Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso. (BRASIL, 2018, art. 9º)

A qualidade de dados garante "[...] aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;" (BRASIL, 2018, art. 6º).

Os dados pessoais devem ter veracidade, portanto, sendo direito do titular de corrigi-los por meio do *habeas data*, quando não estão de acordo com a realidade sendo obrigação do controlador de mantê-los sempre atualizado, observando o mínimo essencial:

> A garantia aqui prevista pretende que o titular tenha seus dados sempre atualizados e corretos podendo o controlador sofrer sanções administrativas caso não os mantenha atualizados ou se negue a corrigir dados equivocados (TEIXEIRA, ARMELIN, 2019, p. 48)

A transparência é o princípio pelo qual o tratador de dados deve identificar os seus agentes, facilitando aos titulares o acesso à informação sobre tais agentes e do próprio tratamento, sendo um princípio ligado diretamente ao livre acesso. Contudo, limita-se aos segredos industriais do controlador.

Segundo o artigo 6º, VII, da lei 13.709/18, o princípio da segurança pode ser conceituado como a:

> 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; (BRASIL, 2018, art. 6º, VII)

A segurança obriga os agentes a terem um sistema apto a proteger os dados pessoais de qualquer acesso não autorizado, além de impedir que eventuais dados venham a ser destruídos, alterados ou difundidos (art. 46, lei 13.709/18).

Portanto, é uma obrigação do controlador de utilizar as técnicas mais avançadas e aplicar os recursos necessários para garantir a segurança, dependendo da importância dos dados. Ademais, caso ocorra a quebra da segurança a empresa

responsável deverá tomar medidas para reduzir os danos do vazamento, da destruição ou difusão de dados pessoais:

> O princípio da segurança, assim como previsto no GDPR, prevê que os agentes, de acordo com as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos de probabilidade e gravidade variável para os titulares também deverão aplicar medidas técnicas e organizativas para assegurar um nível de segurança adequado ao risco, mitigando, assim, as hipóteses de data breach (violação de dados, em português), bem como, caso ocorra algum incidente, que os efeitos colaterais sejam reduzidos. (VAINZOF, 2018, p. 80-81)

Pela prevenção a empresa deverá "[...] conhecer onde está o tratamento de dados, as vulnerabilidades e as prioridades de tratamento [...]" (TEIXEIRA, ARMELIN, 2019, p. 50), dessa forma, tal princípio é mais uma obrigação imposta visando impedir eventuais incidentes. A empresa que trata dos dados pessoais deve sempre estar atualizando o seu sistema de defesa e fortalecendo eventuais brechas.

A não discriminação é fundado no princípio da isonomia, e garante que nenhum dado seja utilizado para "[...] fins discriminatórios ilícitos ou abusivos;" (Brasil, 2018, art. 6º, IX).

Por fim o princípio da responsabilização e prestação de contas está ligado a adoção de medidas para comprovar a observância e o cumprimento das normas de proteção de dados, daí vem algumas das responsabilidades dos agentes de tratamento (art. 37 e 46 da LGPD), isso devido ao grande valor dos dados pessoais.

4.4 Responsabilidade Civil na Lei De Geral De Proteção De Dados Pessoais

A responsabilidade civil é um instituto que serve principalmente para reestabelecer o *status quo ante* ou punir o agente que causa dano a outro. Nesse sentido, trata-se de um instituto fundamental no nosso ordenamento.

O termo responsabilidade surgiu do termo latino *respondere*, de *spondeo*, nascida "[...] de uma obrigação primitiva e de natureza contratual, pela qual o devedor se vinculava ao credor nos contratos verbais." (TARTUCE, 2018, s.p), sendo conceituado como um "Dever jurídico a todos impostos de responder por ação ou omissão imputável que signifique lesão ao direito de outrem, protegido por lei" (GUIMARÃES, 2016, p. 639).

Dessa forma a responsabilidade civil é um instituto que visa a reparação de danos causados por ato cometido pela mesma pessoa (art. 927, Código Civil), por terceiros (art. 932, Código Civil) ou por coisa (art. 936 e 937, Código Civil), objetivando a reparação do dano material ou moral causados ao ofendido (art. 186, Código Civil):

> A responsabilidade civil é a aplicação de medidas que obriguem uma pessoa a reparar dano moral ou patrimonial causado a terceiros, em razão de ato por ela mesma praticado, por pessoa por quem ela responde, por alguma coisa a ela pertencente ou de simples imposição legal (DINIZ, 2018, p. 51)

Ainda:

> [...] podemos definir a responsabilidade civil como a obrigação patrimonial de reparar o dano material ou compensar o dano moral causado ao ofendido pela inobservância por parte do ofensor de um dever jurídico legal ou convencional (MELO, 2015, p. 2)

Nesse liame, mostra-se como um instituto de grande importância no ordenamento jurídico Brasileiro, sendo um mecanismo para restaurar o *status quo ante* e ao mesmo tempo punir os responsáveis.

Para a caracterização de responsabilidade serão necessários três elementos: “a) Existência de uma ação, comissiva ou omissiva [...] b) Ocorrência de um dano moral e/ou patrimonial [...] c) Nexo de causalidade entre o dano e a ação” (DINIZ, 2018, p. 53-54).

Contudo, o estabelecimento destes elementos não é pacifico na doutrina, havendo aqueles que acrescentam a culpa ou dolo do agente:

> b) Culpa ou dolo do agente – Todos concordam em que o art. 186 do Código Civil cogita do dolo logo no início: “ação ou omissão voluntária”, passando, em seguida, a referir-se à culpa: “negligência ou imprudência (GONÇALVES, 2016, p. 53)

Tais elementos vinculados dão origem à responsabilidade civil subjetiva, ou seja, leva-se em consideração a culpa ou dolo do agente causador do dano. Nesse sentido, a responsabilidade civil objetiva é aquela que não leva em conta a culpa ou dolo do agente (art. 927, parágrafo único, Código Civil):

> Art. 927 [...]: Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a

> atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem. (BRASIL, 2001, art. 927).

Um excelente exemplo da utilização da responsabilidade objetiva são as relações consumeristas. O próprio Código de Defesa do Consumidor em seu artigo 14 exclui a necessidade da caracterização de culpa do agente, isso devido aos riscos que os consumidores são expostos:

> Na verdade, o CDC adotou expressamente a ideia da teoria do risco-proveito, aquele que gera a responsabilidade sem culpa justamente por trazer benefícios, ganhos ou vantagens. Em outras palavras, aquele que expõe ao risco outras pessoas, determinadas ou não, por dele tirar um benefício, direto ou não, deve arcar com as consequências da situação de agravamento. Uma dessas decorrências é justamente a responsabilidade objetiva e solidária dos agentes envolvidos com a prestação ou fornecimento. (TARTUCE, 2018, s.p)

A responsabilidade objetiva é fundada na ideia do consumidor ser vulnerável e hipossuficiente frente aos produtores e prestadores de serviços, tal fato também justificaria a exceção que o Código de Defesa do Consumidor faz aos profissionais liberais, que serão responsabilizados subjetivamente (art. 14, §4º, Código de Defesa do Consumidor):

> A norma é justificada, visto que os profissionais liberais individuais, assim como os consumidores, estão muitas vezes em posição de vulnerabilidade ou hipossuficiência. (TARTUCE, 2018, s.p)

A lei observa a vulnerabilidade e os riscos que o consumidor é exposto, além da superioridade apresentada pelos produtores e prestadores de serviços, optando por dar maior proteção ao consumidor, tornando a responsabilidade objetiva em regra, enquanto a subjetiva seria uma exceção.

O mesmo raciocínio pode ser aplicado aos titulares dos dados pessoais. Mesmo que a Lei Geral de Proteção de Dados Pessoais não descreva explicitamente a natureza da responsabilidade civil, a mesma será objetiva.

Conforme visto no tópico 2.3 do presente trabalho, os titulares dos dados pessoais são considerados hipervulneráveis, vez que por muitas vezes não sabem que seus dados estão sendo coletados, graças à tecnologia aplicada na mineração de dados, ou quando sabem não tem consciência do valor destes dados.

Além disso, pela importância dos dados pessoais, os controladores exercem uma atividade que expõe os titulares à determinados riscos. Nesse sentido

a lei 12.414 de 2011, consolidou em seu artigo 16 a regra da responsabilidade objetiva para atividades consideradas de risco, *in verbis*:

> Art. 16. O banco de dados, a fonte e o consulente são responsáveis, objetiva e solidariamente, pelos danos materiais e morais que causarem ao cadastrado, nos termos da Lei nº 8.078, de 11 de setembro de 1990 (Código de Proteção e Defesa do Consumidor). (Brasil, 2011, art. 16)

Ainda:

> O art. 16 da Lei 12.414/2011, também consolida um entendimento há muito pacificado no nosso ordenamento, segundo o qual os danos materiais e morais causados pelas atividades de risco devem ser reparados no âmbito de um sistema de responsabilidade objetiva e solidária. (MENDES, 2018, p. 16)

Para que haja reparação de danos materiais e morais provenientes de danos causados pela violação à proteção de dados pessoais, será necessário estabelecer a responsabilidade objetiva como regra na lei geral de proteção de dados:

> Para a reparação dos danos morais e materiais advindos da violação do direito fundamental à proteção de dados, faz-se necessária a aplicação de um sistema de responsabilidade objetiva e solidária (MENDES, 2018, p. 24)

Segundo interpretação do artigo 42 da LGPD, ao vincular a obrigação de reparação dos danos com o exercício do tratamento de dados pessoais, o legislador demonstra a opção pela objetividade da responsabilidade:

> Assim justifica-se o legislador optar por um regime de responsabilidade objetiva no art. 42, vinculando a obrigação da reparação do dano ao exercício de atividade de tratamento de dados pessoais. (MENDES, 2018, p. 05)

Seguindo este raciocínio, o artigo 43 da LGPD descreve as situações em que os agentes de tratamento não serão responsabilizados, tais situações são semelhantes às descritas pelo artigo 12, §3º do Código de Defesa do Consumidor.

Sabe-se que o Código de Defesa do Consumidor e a Lei Geral de Proteção de Dados visam proteger o consumidor e o titular dos dados, devido a vulnerabilidade de cada um, o que justifica a semelhança entre os dispositivos, ademais outro ponto que prova tal similaridade seria a aplicação da responsabilidade

objetiva em ambos os diplomas, o que fundamenta também a aplicação análoga do Código de Defesa do Consumidor.

Pode-se concluir que a aplicação do sistema de responsabilização objetiva é o mais adequado, visto que os titulares dos dados podem ser considerados hipervulneráveis, fazendo assim uma analogia com a responsabilidade objetiva do Código de Defesa do Consumidor, além disso, visto a grande importância dos dados pessoais, as atividades de processamento expõem a figura do titular à riscos, o que justifica maior proteção.

4.4.1 Responsabilidade Dos Agentes De Tratamento de Dados

A princípio será necessário discutirmos as obrigações impostas a cada agente de tratamento de dados, para posteriormente estudarmos a responsabilidade de cada um. A primeira obrigação prevista na lei 13.709/15 é a observância dos princípios estabelecidos pela própria lei, conforme cita o artigo 7º, §6º:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> [...] § 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.
> [...] § 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular. (Brasil, 2018, art. 7)

Logo, aos casos em que os dados já forem manifestamente públicos não será necessário o consentimento do titular para o tratamento destes dados, contudo, ainda será necessário seguir os princípios estabelecidos pela lei[58].

O artigo 7 tem sua devida importância pois estabelece as hipóteses em que poderá ocorrer o tratamento de dados pessoais, o dispositivo traz dez incisos autoexplicativos, contudo, há um em especial que merece a devida atenção. Trata-se do inciso IX:

> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades

[58] Eis um interessante exemplo normativo da diferença entre o direito a proteção de dados pessoais e o direito a privacidade trabalhado no capítulo II.

> fundamentais do titular que exijam a proteção dos dados pessoais; ou [...] (Brasil, 2018, art. 7, IX)

O inciso traz a figura do legitimo interesse do controlador, que confere ao mesmo uma grande variedade de hipóteses para tratamento de sua base de dados. A utilização destes dados, sob o legitimo interesse, pode ser fundamentada no "[...] apoio e promoção das atividades do controlador; e [...] proteção do banco de dados" (Brasil, 2018, art. 10), havendo outras hipóteses não descritas pela lei. Salienta-se que o próprio artigo 10, em seus parágrafos, estabelece limites ao legitimo interesse.

Daí decorre o dever do operador e do controlador de "[...] manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse." (Brasil, 2018, art. 37)

Os agentes devem manter sua rede e banco de dados protegidos, adotando medidas de segurança, técnicas e administrativas, que sejam aptas a proteger os dados coletados:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. (Brasil, 2018, art. 46)

Nessa situação a própria lei já imputa a responsabilidade aos agentes pela falta de segurança:

> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:
> [...] Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

Além disso, é dever dos agentes de tratamento, e de qualquer outro que tenha intervindo em alguma das fases de tratamento, garantir a segurança dos dados, mesmo após o término do tratamento:

> Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término. (Brasil, 2018, art. 47)

Em relação às obrigações especificas de cada agente, o controlador deve prestar informações ao titular dos dados a qualquer momento, mediante requisição:

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição (Brasil, 2018, art. 18)

Além disso, quando houver algum incidente de segurança, deverá comunicar imediatamente a autoridade nacional e fazer um relatório acerca dos dados comprometidos e das atitudes tomadas:

> Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
> § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo: I - a descrição da natureza dos dados pessoais afetados; II - as informações sobre os titulares envolvidos; III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; IV - os riscos relacionados ao incidente; V - os motivos da demora, no caso de a comunicação não ter sido imediata; e VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. (Brasil, 2018, art. 48)

Pode-se entender que os agentes tem as seguintes obrigações: observar os princípios e garantias do titular (art. 7, §6); fazer registros das operações, principalmente quando estiverem atuando em legitimo interesse (art. 37); adotar medidas de segurança, técnicas e administrativas (art. 46) e assegurar os dados mesmo após o termino do tratamento (art. 47), sendo que o controlador ainda tem a obrigação de prestar informações ao titular (art. 18) e de comunicar a autoridade nacional acerca de eventual incidente (art. 48).

A necessidade de estudar as obrigações dos agentes se justifica no momento em que o artigo 42[59] da LGPD, impõe que:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:

[59] A possibilidade de danos morais, individuais ou coletivos, fundamenta o direito a proteção de dados como um direito personalíssimo.

> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei. [...] (Brasil, 2018, Art. 42, Grifo nosso)

Segundo o art. 42, §1º, I, o operador só responderá solidariamente, quando vier a descumprir as obrigações da legislação de proteção de dados, ou quando não obedecer às ordens lícitas do controlador. Enquanto o controlador responderá solidariamente, na hipótese em que o tratamento que estava diretamente envolvido cause danos ao titular (art. 42, §1, II), ou seja, bastaria a sua participação para responsabilização.

Percebe-se que a responsabilidade aplicada ao operador é diferente da aplicada ao controlador, vez que é atrelado ao descumprimento dos preceitos legais ou do descumprimento de ordens, sendo caracterizado por alguns de "responsabilização *sui generis*" (TEIXEIRA; ARMELIN, 2019, p. 118).

Contudo, há hipóteses em que a responsabilidade de qualquer agente será excluída, tratamos das situações vinculadas no artigo 43:

> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem: I - que não realizaram o tratamento de dados pessoais que lhes é atribuído; II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro. (Brasil, 2018, art. 43)

A primeira hipótese (art. 43, I) cita que os agentes que não realizaram o tratamento não serão responsabilizados, claramente porque não há uma conduta praticada pelo agente que tenha nexo causal com o dano.

A segunda situação, descrita pelo inciso II, assegura que se o agente seguiu todos os preceitos estabelecidos pela Lei Geral de Proteção de Dados Pessoais, não será punido, caso "[...] ausente qualquer ilicitude, mesmo que tenha tratado os dados pessoais [...]" (TEIXEIRA; ARMELIN, 2018, p.121).

A excludente mais interessante para o presente trabalho se encontra no inciso III, que trata do dano exclusivo do titular ou de terceiros. Nessa situação os agentes de processamento devem provar que cumpriram com todos os requisitos de

segurança – daí a fundamentação do inciso III, do §1º, do artigo 48, LGPD – e que não houve nenhum desrespeito aos dispositivos da lei.

Em todas estas situações, como manda o artigo 42, §2º, da LGPD, haverá a inversão do ônus da prova quando "[...] houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa." (Brasil, 2018, art. 42). A prova pelo agente poderá ser feita pelos documentos que este é obrigado a registrar (art. 37, LGPD), conforme o princípio da prestação de contas.

Além disso, em relação ao caso fortuito e força maior, o Código Civil em seu artigo 393 cita:

> Art. 393. O devedor não responde pelos prejuízos resultantes de caso fortuito ou força maior, se expressamente não se houver por eles responsabilizado. Parágrafo único. O caso fortuito ou de força maior verifica-se no fato necessário, cujos efeitos não era possível evitar ou impedir. (BRASIL, 2002, art. 393, grifo nosso).

O artigo nos indica a possibilidade de exclusão de responsabilidade nestes casos. Contudo, tal excludente deve ser analisada cuidadosamente, tendo em vista que a exclusão só será aplicada caso o agente não tenha assumido a responsabilidade por tais situações.

Ocorre que na Lei Geral de Proteção de Dados Pessoais, pelo princípio da segurança, é dever dos agentes de tratamento "[...] proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;" (Brasil, 2019, art. 6º, VII).

Ou seja, em se tratando de um princípio atribuído pela lei, automaticamente os agentes de tratamento serão responsabilizados por eventuais fortuitos que ocorrerem durante o tratamento de dados.

Salienta-se que atualmente a tecnologia de backup em nuvens é muito comum e segura, logo, em situações de destruição fortuita do *hardware* que continha os dados pessoais, a excludente de caso fortuito não poderá ser arguida.

Por fim, os agentes poderão sofrer sanções administrativas, caso deixem de cumprir com as suas obrigações, é o que cita o artigo 52 da LGPD.

4.4.2 Responsabilidade Civil Do Vazamento De Dados Pessoais Por Ataques De *Crackers*

É muito recorrente encontrar nos noticiários casos de ataques cibernéticos à bancos de dados, muitas vezes os *crackers* têm a finalidade de conseguir vantagens indevidas, como já foi visto, tais figuras poderão ser processadas criminalmente.

Permanece a dúvida acerca da responsabilidade civil dos agentes quando ocorre esse tipo de ataque. Assim, será analisada tal hipótese e para tanto valer-se-á de casos reais e suas consequências jurídicas, contudo, cabe salientar que estaremos baseando nossos estudos em fatos relatados pela imprensa ou por documentos públicos.

A segurança dos dados pessoais é uma obrigação tanto para o controlador quanto para o operador (art. 46, LGPD), nesse sentido a falha da segurança dos bancos de dados será de responsabilidade dos mesmos.

Não será possível, nessa situação, a aplicação da excludente de ilicitude do artigo 43, III, da Lei Geral de Proteção de Dados, pois a própria lei já imputa responsabilidade pela falta de segurança (art. 44, LGPD). Logo, a única forma de se aplicar a excludente por fato de terceiro, será no caso de ser provado que não houve nenhuma falha, e que o operador e o controlador adotaram as medidas técnico e administrativas de segurança.

Um excelente caso é o do Banco Inter, que sofreu ataques cibernéticos e tiveram os dados pessoais de cerca de “13.207 (treze mil duzentos e sete) contas/clientes com dados bancários comprometidos (folhas 72-75 dos autos sigilosos).” (CEROY, 2018, p. 08), isso graças a uma falha de segurança que deu aos *crackers* acesso às chaves digitais do banco em 2018.

A inicial que o Ministério Público do Distrito Federal e Regiões (MPDFT) propôs em face do Banco Inter, baseou-se no Código de Defesa do Consumidor (Súmula 297 do Superior Tribunal de Justiça), e se fundou nas análises que o Banco Central do Brasil e o Centro de Produção, Análise, Difusão e Segurança da Informação – CI apresentaram:

> O Banco Central do Brasil confirmou o incidente de segurança, bem como o Centro de Produção, Análise, Difusão e Segurança da Informação – CI deste Ministério Público constatou que os certificados contidos no arquivo são

> relativos ao Banco Inter e são compatíveis com as chaves pública e privada. (CEROY, 2018, p. 14)

Nesse sentido, o MPDFT pleiteou o valor de R$ 10.000.000,00 (dez milhões de reais) à título de danos morais coletivos, todavia, o processo foi extinto graças ao acordo realizado entre o banco e o Ministério Público:

> Justiça homologou, nesta terça-feira, 18 de dezembro, acordo entre o Ministério Público do Distrito Federal e Territórios (MPDFT) e o Banco Inter. A instituição bancária pagará R$ 1,5 milhão como forma de reparar os danos morais coletivos de caráter nacional decorrentes do vazamento de dados de mais de 19 mil correntistas. (BANCO Inter: Acordo Destinará R$ 1,5 milhão para caridade e combate a crimes cibernéticos).

Outro ponto a ser destacado é que o Banco Inter não deu informações acerca do incidente de segurança:

> Em resposta datada de 10 de maio de 2018 (fls. 31/37), o Banco Inter S/A informou que não houve danos a seus clientes, bem como não foi identificada fraude ou uso indevido relacionado ao incidente, negando-se a responder aos questionamentos deste Órgão Ministerial. Na oportunidade, informou que já havia dado ciência dos fatos ao Banco Central e à Polícia Federal. (CEROY, 2018, p. 04)

Interessante notar que se o caso tivesse ocorrido durante a vigência da Lei Geral de Proteção de Dados Pessoais, teríamos o seguinte quadro de responsabilização:

O Banco Inter, como pessoa jurídica, será responsabilizado objetivamente, pois o tratamento de dados pessoais é uma atividade de risco e expõe os titulares. O Controlador, pessoa física ou pessoa jurídica, será responsabilizado solidariamente se tiver participado do tratamento diretamente (art. 42, II, Lei Geral de Proteção de Dados Pessoais). O operador só responderá solidariamente se deixou de cumprir com a legislação de proteção de dados pessoais ou não tiver seguido as instruções lícitas do controlador (art. 42, I, Lei Geral de Proteção de Dados Pessoais).

Logo, eventuais danos materiais e morais decorrentes do fato lesivo serão de responsabilidade destas três figuras, caso não coincidentes. Os agentes ainda sofrerão as sanções administrativas do artigo 52 da LGPD, principalmente pelo controlador que supostamente teria deixado de comunicar a agencia nacional.

Um segundo caso, um tanto semelhante, foi a invasão que a empresa Uber sofreu, comprometendo os dados de milhares de motoristas e usuários. Não se

sabe a época em que ocorreram os ataques, tendo em vista que a empresa supostamente pagou aos *crackers* para apagarem os dados obtidos:

> Yet the note and Uber's eventual $100,000 payment to the hacker, which was initially celebrated internally as a rare win in corporate security, have since turned into a public relations debacle for the company. [60] (PERLROTH; ISAAC, 2018, s.p)

Contudo, o incidente ainda foi exposto, constatando que os usuários afetados são de diversos países, sendo que foram cerca de "[...] 196 mil usuários brasileiros atingidos pelo incidente de segurança tornado público no final de 2017." (UBER termina de notificar usuários brasileiros afetados por vazamento de dados).

Após acordo com o MPDFT a empresa teve de notificar todos os usuários e motoristas brasileiros acerca do vazamento de dados:

> Após acordo firmado com a Comissão de Proteção dos Dados Pessoais do Ministério Público do Distrito Federal e Territórios (MPDFT) no início de abril, a empresa Uber terminou de notificar, nesta quinta-feira, 26 de abril, os mais de 196 mil usuários brasileiros atingidos pelo incidente de segurança tornado público no final de 2017. A comunicação foi feita por mensagem enviada aos e-mails cadastrados na plataforma da empresa. (UBER termina de notificar usuários brasileiros afetados por vazamento de dados)

Todas as sanções aplicáveis ao caso do Banco Inter poderiam ser aplicadas ao caso da Uber, contudo, há o fato da empresa ter pagado aos *crackers* para apagarem os dados obtidos, ou seja, além de acobertar o incidente, pagaram para destruir as provas do vazamento.

5. CONCLUSÃO

Observou-se ao longo do trabalho que os dados pessoais ganharam grande relevância no mercado e na sociedade, da mesma forma, o ordenamento jurídico teve de se adaptar para proteger os dados pessoais.

Um dos grandes dilemas que rodeiam o tema é o conceito dos tais "dados pessoais". A sua definição é um grande limitador da tutela legal oferecida pela

[60] Apesar da nota e o eventual pagamento de US $ 100.000 da Uber ao *hacker*, que inicialmente foi comemorado internamente como uma rara vitória na segurança corporativa, transformaram-se em um desastre de relações públicas para a empresa. (Tradução Nossa)

lei 13.079/19 (LGPD), daí vem a importância de sua discussão. Nesse sentido pode-se dizer que os dados pessoais são aqueles atrelados à uma pessoa física, identificada ou identificável (desde que respeite a razoabilidade dos meios de desanonimização), podendo ser incluído neste conceito os dados utilizados para formação de perfis comportamentais, seguindo assim a tendência expansionista do conceito.

Tal conceito é o mais adequado para o nosso ordenamento, pois garante uma tutela maior sobre os dados pessoais, sendo limitado pelo princípio da razoabilidade já concretizado no Brasil.

Os dados pessoais podem ser considerados como peças de um grande quebra cabeça, que se montado, forma uma biografia do titular, então na situação em que alguém coleta dados de várias fontes (*Facebook, Instagram, Twitter, Snapchat, Linkedin...)* e os junta, formará a identidade digital do titular. Dessa forma, entende-se que a proteção de dados pessoais é um direito personalíssimo, tal entendimento é reforçado quando estudamos os fenômenos da datificação e do *proffiling*.

A utilização destes dados pelos grandes *players* acaba se tornando um excelente instrumento para manipular as massas e influenciar decisões. Fato que é agravado no momento em que o usuário não tem noção de que seus dados estão sendo coletados, ou quando sabe, não dá a devida importância aos mesmos, o que os tornam hipervulneráveis.

Nesse sentido a proteção de dados pessoais deve ser concretizada, buscando-se uma maior abrangência, logo, existe a necessidade de se positivar tal direito no texto constitucional, contudo, não ser confundido com o direito à privacidade, vez que a proteção de dados trata de institutos que tutelam liberdades diversas.

Percebe-se, assim, que a positivação da proteção de dados no corpo constitucional pode ser uma ideia imatura, pois, trata-se de um instituto pouco discutido (até certo ponto), e quando é, assume a forma de uma dimensão do direito à privacidade.

Visando aumentar a tutela sobre os dados pessoais, em 2018, foi aprovado a lei 13.709/2018, a Lei Geral de Proteção de Dados Pessoais que entrará em vigor em agosto de 2020. É um importante marco para a proteção de dados no ordenamento brasileiro, vez que era necessária uma lei especifica para tratar de um tema tão técnico.

A lei não cita expressamente o sistema de responsabilidade civil a ser aplicada aos agentes de tratamento de dados pessoais, porém, ante a hipervulnerabilidade do titular, é indiscutível que seja objetiva.

Assim, percebe-se uma certa semelhança com o Código de Defesa do Consumidor, que em sua premissa assume a responsabilidade objetiva no intuito de defender o consumidor que está em uma posição de vulnerabilidade frente ao produtor e prestador de serviços, tanto que as causas de excludentes de responsabilidade dispostas em ambos os diplomas são análogas, o que justifica a aplicação da responsabilidade objetiva em ambas as leis.

Conclui-se que os agentes de tratamento de dados pessoais responderão de maneira diversas, o operador terá uma responsabilidade *sui generis*, dependendo da obediência das ordens lícitas do seu controlador e da observância dos preceitos estipulados pela lei. Já em relação ao controlador bastaria a sua participação direta no tratamento que gerou os danos, aproximando-se assim da responsabilidade objetiva.

No caso do descumprimento de alguma das obrigações impostas ao controlador e ao operador, também poderão ser aplicadas sanções em âmbito administrativo.

Por fim, na hipótese de vazamento de dados pessoais por ataque *hacker* a responsabilidade atribuída aos agentes de tratamento fundamenta-se nas conclusões tecidas anteriormente, porém, salienta-se a impossibilidade da alegação de culpa exclusiva de terceiros, pois a própria lei já impõe como uma obrigação a manutenção da segurança dos bancos de dados.

REFERÊNCIAS

ALEMANHA. **Federal Data Protection Act of 30 june 2017.** Disponível em: https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html#p0014. Acesso em: 29 de março de 2019.

ALVES, Paulo. **O que são cookies? Entenda os dados que os sites guardam sobre você**. Site da TECHTUDO, 04 de outubro de 2019. Disponível em:

https://www.techtudo.com.br/noticias/2018/10/o-que-sao-cookies-entenda-os-dados-que-os-sites-guardam-sobre-voce.ghtml. Acesso em 04 de maio de 2019.

BANCO Inter: acordo destinará R$ 1,5 milhão para caridade e combate a crimes cibernéticos. **Site do Ministério Público do Distrito Federal**. Publicado em 19 de dezembro de 2018. Disponível em: http://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2018/10524-2018-12-19-10-27-31. Acesso em: 01 de outubro de 2019.

BAROCAS, Solon; NISSENBAUM, Helen F., **On Notice: The Trouble with Notice and Consent (2009)**. Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information, outubro de 2009. Disponível em: https://ssrn.com/abstract=2567409. Acesso em 02 de maio de 2019.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** a função e os limites do consentimento. Ed 1. Vol. Único. Rio de Janeiro: Forense, 2019

_____. **Xeque-Mate:** o tripé de dados pessoais das iniciativas legislativas Brasileiras. São Paulo: GPoPAI/USP (Grupo de Pesquisa em políticas públicas para acesso à informação da USP), 02 de julho de 2015.

_____. **Bruno Bioni:** Whatsapp e a chance para uma nova discussão? Portal de Telecomunicações, Internet e TICs, 04 de outubro de 2016. Disponível em: http://www.telesintese.com.br/nova-politica-de-privacidade-do-whatsapp-chance-de-se-discutir-modelos-de-negocios-e-praticas-de-tratamento-de-dados-menos-invasivos-privacidade/. Acesso em 30 de abril de 2019.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 02 de outubro de 2019.

_____. **Lei nº 10.406, de 10 de janeiro de 2002.** Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406.htm. Acesso em: 02 de outubro de 2019.

_____. **Decreto-lei nº 2.848, de 7 de novembro de 1940.** Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 02 de outubro de 2019.

_____. **Lei nº 9.507, de 12 de novembro de 1997.** Regula o direito de acesso a informações e disciplina o rito processual do habeas data. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L9507.htm. Acesso em: 02 de outubro de 2019.

_____. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 28 de setembro de 2019.

_____. **Lei nº 12.414, de 09 de junho de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm. Acesso em 28 de setembro de 2019.

_____. Senado Federal. **Projeto de Emenda Constitucional nº 17 de 2019. Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria.** Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7924709&ts=1564052658848&disposition=inline. Acesso em 07 de agosto de 2019.

BURN-MURDOCH, John. **Big data:** what is it and how can it help?. Site The Guardian, 26 de outubro de 2012. Disponível em: https://www.theguardian.com/news/datablog/2012/oct/26/big-data-what-is-it-examples. Acesso em 18 de junho de 2019.

CANOTILHO, José Joaquim. **Direito Constitucional**. 6ª Ed. Vol. Único. Coimbra: Livraria Almedina, 1993.

_____. **CRP Constituição da República Portuguesa Anotada**. Volume 1, artigos 1º a 107. Ed. 1. São Paulo: Revista dos Tribunais, 2007.

CASTELLS, Manuel. **A Sociedade em Rede**. São Paulo: Paz e Terra, 2006.

CEROY, Frederico Meinberg. **Ação Civil Pública por Danos Morais Coletivos em desfavor do Banco Inter S/A.** Proposta em 30 de julho de 2018. Disponível em: http://www.mpdft.mp.br/portal/pdf/noticias/dezembro_2018/ACP_-_Banco_Inter.pdf. Acesso em: 01 de outubro de 2019.

CHILE. **Constituição Política da República do Chile de 2005**. Disponível em: https://www.leychile.cl/Navegar?idNorma=242302&idParte=&idVersion=. Acesso em: 13 de agosto de 2019.

COOKIES – O que são e como excluir. **Site da Mozilla Firefox.** Disponível em: http://br.mozdev.org/firefox/cookies. Acesso em: 04 de maio de 2019.

COSTA JR. Paulo José da. **O direito de estar só:** tutela penal da intimidade. 4. ed. São Paulo: Ed. RT, 2007, p. 10-11.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Ed. 1. Vol. Único. Rio de Janeiro: Renovar, 2006.

_____. **A PROTEÇÃO DOS DADOS PESSOAIS COMO UM DIREITO FUNDAMENTAL.** Espaço Jurídico. V. 12, n. 2, 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315/658. Acesso em 07 de outubro de 2019.

DIJCK, José Van. **Confiamos nos dados? As Implicações da datificação para o monitoramento social**. Revista da USP. V. 11 – nº 1º: Jan/abr. 2017.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro. Responsabilidade Civil.** Ed. 32. Vol. 7. São Paulo: Saraiva, 2018.

ENTENDA o ataque à rede on-line do Playstation 3, a PSN. **Site do G1.** De 09 de maio de 2011. Disponível em: http://g1.globo.com/tecnologia/noticia/2011/05/entenda-o-ataque-rede-line-do-playstation-3-psn.html. Acesso em: 29 de junho de 2019.

ENTENDA o escândalo de uso político de dados que derrubou o valor do Facebook e o colocou na mira de autoridades. **Site do G1.** De 20 de março de 2018. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml. Acesso em: 16 de novembro de 2019.

ESPANHA. **Constituição Espanhola de 1978.** Disponível em: https://www.tribunalconstitucional.es/es/tribunal/normativa/Normativa/CEportugu%C3%A9s.pdf. Acesso em 13 de agosto de 2019.

EUROPA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.** Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT. Acesso em 03 de abril de 2019.

_____. ***General Data Protection Regulamentation. Regulamento2016/679 de 27 de abril de 2016.*** Disponível em: http://portaldaprivacidade.com.br/wp-content/uploads/2018/05/GDPR-Corrigendum-em-portugu%C3%AAs.pdf. Acesso em: 03 de abril de 2019.

GONÇALVES, Carlos Roberto. **Direito civil brasileiro, volume 4:** responsabilidade civil / Carlos Roberto Gonçalves. Ed. 12. São Paulo: Saraiva, 2017.

GUIMARÃES, Deocleciano Torrieri. **Dicionário Técnico Jurídico**. Ed. 19. Vol. Único. São Paulo: Rideel, 2016.

HESSE, Konrad. **Significado de los derechos fundamentales.** Manual de derecho constitucional. Ernst. Benda, Werner Maihofer, Hans-Jochen Vogel et elli. 2. Ed. Madrid: Marcial Pons, 2001.

HOUAISS, Antônio. **Dicionário Houaiss da Língua Portuguesa***.* Rio de Janeiro, Ed. Objetiva, 2001.

HTML5 Web Storage. **Site da W3SCHOOLS.**Disponível em: https://www.w3schools.com/html/html5_webstorage.asp. Acesso em 11 de maio de 2019

IBM. **Você realmente sabe o que é Big Data?**. 30 de abril de 2012. Disponível em: https://www.ibm.com/developerworks/community/blogs/ctaurion/entry/voce_realmente_sabe_o_que_e_big_data?lang=en. Acesso em: 04 de maio de 2019.

ITS (INSTITUTO DE TECNOLOGIA & SOCIEDADE DO RIO). **Big Data no projeto Sul Global. Relatório de estudos.** Rio de Janeiro: 2016. Disponível em: https://itsrio.org/wp-content/uploads/2017/01/ITS_Relatorio_Big-Data_PT-BR_v2.pdf. Acesso em: 06 de maio de 2019.

LOPES, Alan Moreira (Coord.); TEIXEIRA Tarcísio (Coord.); TAKADA, Thalles (Coord.). **Manual Jurídico da inovação e das startups**. Ed. 1. Vol. Único. Salvador: Editora Juspodvim, 2019.

MARQUES, Marília. MP do DF aponta suposto esquema de venda de dados pessoais de brasileiros pelo Serpro. **Site do G1**, 2018. Disponível em: https://g1.globo.com/df/distrito-federal/noticia/mp-do-df-aponta-suposto-esquema-de-venda-de-dados-pessoais-de-brasileiros-pelo-serpro.ghtml. Acesso em 04 de outubro de 2019.

MARTÍ, Silas. Entenda o escândalo do uso de dados do Facebook. Informações foram utilizadas para influenciar na eleição de Trump. **Folha de São Paulo**. São Paulo: 22 de março de 2018. Disponível em: https://www1.folha.uol.com.br/mercado/2018/03/entenda-o-escandalo-do-uso-de-dados-do-facebook.shtml. Acesso em 04 de outubro de 2019.

MARTINS, Guilherme Magalhães. **Responsabilidade por acidente de consumo na Internet**. Revista de Direito do Consumidor Vol. 78/2011.São Paulo: Revista dos Tribunais, 2008.

MARTINS, Leonardo. **Cinquenta anos da Jurisprudência do Tribunal Constitucional Federal Alemão.** Organização e introdução: Leonardo Martins. Prefácio: Jan Wischnik. Tradução de Beatriz Hennig, Leonardo Martins, Mariana Bigelli de Carvalho, Tereza Maria de Castro e Vivianne Geraldes Ferreira. KONRAD-ADENAUER-STIFTUNG E.V: 2005.

MASSENO, Manuel David. **Formação Data Protection Officer (DPO)**. Os fundamentos e as fontes, 28 de maio de 2018.

_____. **On the Criminalization of Hacking a look at the European (COE & EU) Legal Framework**. Sem data.

MASSON, Cléber. **Direito Penal Esquematizado: Parte Especial (arts. 121 a 212).** Vol. 2. Ed. 9ª. Rio de Janeiro: Forense/ São Paulo: Método, 2016.

MAYER-SCHÖNBERGER, Viktor. **Generational development of data protection in Europe.** In: AGRE, Philip E.; ROTENBERG, Marc. Technology and privacy: the new landscape. Cambridge: The Mit Press, 2001. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=H2KB2DK4w78C&oi=fnd&pg=PA219&dq=MAYER-SCH%C3%96NBERGER,+Viktor.+Generational+development+of+data+protection+in+Europe&ots=1XYgtaTxJt&sig=Nyb4PudZcrsQTy44I5_mct-SwD0#v=onepage&q&f=false. Acesso em: 09 de março de 2019.

MAYER-SCHONEBERGER, Viktor, CUKIER, Kenneth. **Big data:** A revolution will transform how we live, work and think. New York: Houghton Mifflin Publishing, 2013.

MCAFFE, Andrew; BRYNJOLFSSON, Erik. **Big Data: The Managemente Revolution**. Harvard Business Review, Oct. 2012. Disponível em: https://hbr.org/2012/10/big-data-the-management-revolution. Acesso em: 07 de outubro de 2019.

MELO, Marco Aurélio Bezerra. **Curso de Direito Civil. Responsabilidade civil.** Vol. 4. São Paulo: Atlas, 2015.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. Edição do Kindle. Vol. Único. São Paulo: Saraiva, 2014.

_____. **O direito fundamental à proteção de dados pessoais.** Revista de Direito do Consumidor. Vol. 79/2011. Revista dos Tribunais: Jul-Set, 2011.

_____. **Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados**. Revista de Direito do Consumidor. Vol 120/2018.Nov - dez. Revista dos Tribunais: 2018.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. **Robust De-anonymization of Large Sparse Datasets**.The University of Texas in Austin.Disponível em: https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf. Acesso em: 28 de março de 2019.

NOVELINO, Marcelo. **Direito Constitucional**. Ed. 6. São Paulo: Editora Método, 2012.

OECD. **"Guidelines on the Protection of Privacy and Transborder Flows of Personal Data"** de 11 de julho de 2013. Disponível em:

https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf. Acesso em: 22 de março de 2019.

OHM, Paul. **Broken Promises of Privacy:** Responding to the Surprising Failure of Anonymization. UCLA *Law Review*, v. 57, 2010. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006. Acesso em 28 de março de 2019.

ORRÚ, Romano. **La Constituzione di tutti Il Sudafrica dalla segregazione razziale alla democrazia della «Rainbow nation»**. Vol. Único. Torino: Gianpichelli, 1998.

OXFORD. **Dicionário Online da Oxford University Press, 2019**. Disponível em https://en.oxforddictionaries.com/. Acesso em 22 de março de 2019.

PANEBIANCO, Mario. ***Bundesverfassungsgericht, dignità umana e diriti fondamentali***. In: *Diritto e Società*, n. 2, 2000, p. 151-242.

POLÍTICA de privacidade da Samsung – suplemento da Smart Tv. **Site da Samsung**. Disponível em: https://www.samsung.com/br/info/privacy/smarttv/. Acesso em: 09 de julho de 2019.

PERLROTH, Nicole; ISAAC, Mike. Inside Uber's $100,000 Payment to a Hacker, and the Fallout. **Site do *The New York Times***, 2018. Disponível em: https://www.nytimes.com/2018/01/12/technology/uber-hacker-payment-100000.html. Acesso em: 02 de outubro de 2019.

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais. Comentários à Lei n. 13.709/2018**. Ed. 1. Vol. Único. São Paulo: Saraivajur, 2018.

PORTUGAL. **Constituição da República Portuguesa. Texto originário da Constituição aprovada em 2 de abril de 1976.** Disponível em: https://www.parlamento.pt/parlamento/documents/crp1976.pdf. Acesso em: 22 de abril de 2019.

PRIVACIDADE na internet: conheça os cookies, web beacons e flash cookies. **Site da UOL**. 29 de agosto de 2013. Disponível em: https://seguranca.uol.com.br/antivirus/dicas/curiosidades/privacidade-na-internet-conheca-os-cookies-web-beacons-e-flash-cookies.html#rmcl. Acesso em 11 de maio de 2019.

PROTEÇÃO dos Dados Pessoais, site do **Parlamento Europeu**, disponível em http://www.europarl.europa.eu/factsheets/pt/sheet/157/protecao-dos-dados-pessoais. Acesso em: 23 de abril de 2019.

QUAL a diferença entre hacker e cracker? **Site do Olhar Digital** de 03 de outubro de 2013. Disponível em: https://olhardigital.com.br/fique_seguro/noticia/qual-a-diferenca-entre-hacker-e-cracker/38024. Acesso em 24 de junho de 2019.

ROTUNDO, Rafael Pinheiro. **PROTEÇÃO DE DADOS**. Revista de Direito Privado. Vol. 74/2017. Revista dos Tribunais – fev. 2017.

RUARO, Regina Linden. **O Direito Fundamental à Proteção de Dados Pessoais do Consumidor e Livre Mercado**. Revista de Direito do Consumidor. Vol. 118/2018. Revista dos Tribunais: Jul-Ago, 2018.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**. Porto Alegre: Livraria do Advogado, 2009.

SCHWARTZ, Paul; M. SOLOVE, Daniel J. **The PII Problem**: Privacy and a New Concept of Personally Identifiable Information. Review law 86N.Y.U.L.Q. Rev. 1814, 2011. Disponível em: https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2638&context=facpubs. Acesso em 22 de março de 2019.

SILVA, De Plácio. **Vocabulário jurídico**. 12. ed. Rio de Janeiro: Forense, 1993.

SILVA, Leornardo Werner. **Internet foi criada em 1969 com o nome de "Arpanet" nos EUA.** Folha de São Paulo: 12 de agosto de 2001. Disponível em: https://www1.folha.uol.com.br/folha/cotidiano/ult95u34809.shtml. Acesso em 06 de março de 2019.

SIMITIS, Spiros. II. **Contesto giuridico e político della tutela della privacy**. Rivista Critica Del Diritto Privato, 1997.

SMITH, Russell G.; GRABOSKY, Peter; URBAS, Gregor. **Cyber Criminals on Trial**. Ed. 1. Cambridge: Cambridge University Press, 2004.

SOLOVE, Daniel J. **The Digital person:** technology and privacy in the information age. New York: New York University Press, 2004.

SWEENEY, Latanya. **Simple Demographics Often Identify People Uniquely.** Carnegie Mellon University, Data. Privacy Working Paper 3. Pittsburgh 2000. Disponível em https://dataprivacylab.org/projects/identifiability/paper1.pdf. Acesso em: 01 de abril de 2019.

TARTUCE, Flávio. **Manual de responsabilidade civil: volume único.** Versão digital. Rio de Janeiro: Forense; São Paulo: Método, 2018.

TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei Geral de Proteção de dados pessoais:** comentada artigo por artigo. Vol. Único. Ed. 1. Salvador: Editora Juspodvim, 2019.

TENE, Omer. **Privacy Law's Midlife Crisis: A critical Assessment of the Second Wave of Global Privacy Laws**, *Ohio State Journal, v. 74, 2013*. Disponível em: https://kb.osu.edu/bitstream/handle/1811/71612/1/OSLJ_V74N6_1217.pdf. Acesso em: 01 de abril de 2019.

UBER termina de notificar usuários brasileiros afetados por vazamento de dados. **Site do Ministério Público do Distrito Federal**. Disponível em: https://tecnoblog.net/247956/referencia-site-abnt-artigos/. Acesso em: 02 de outubro de 2019.

VAINZOF, Rony. **Dados Pessoais, Tratamento e Princípios.** In. MALDONADO, Viviane Nóbrega; BLUM, Renato Ópice. Comentários ao GDPR. São Paulo: Thomson Reuters Brasil, 2018.

VIANNA, Túlio Lima. **Hackers:** um estudo criminológico da subcultura cyberpunk. In CERQUEIRA, Tarcísio Queiroz, IRIARTE, Erick, PINTO, Márcio Morena (Coords.). Informática e Internet: aspectos legais internacionais. Rio de Janeiro: Esplanada, 2001.

WARREN, Samuel; BRANDEIS, Louis. **The Right to Privacy**. Harvard Law Review, Vol. 4, Nº 5. Cambridge: Harvard Law Review, 1890.

ZANON, João Carlos. **Direito à Proteção dos Dados Pessoais.** Dissertação (Mestrado em Direito). PUCSP, 2012.