UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO

Maria Elisa Paiva Feitosa de Azevedo Cunha

OS DADOS PESSOAIS COMO O NOVO PETRÓLEO: A ABORDAGEM JURÍDICA DO TRATAMENTO DE DADOS NA ERA DA INFORMAÇÃO

Rio de Janeiro

2018

Maria Elisa Paiva Feitosa de Azevedo Cunha

OS DADOS PESSOAIS COMO O NOVO PETRÓLEO: A ABORDAGEM JURÍDICA DO TRATAMENTO DE DADOS NA ERA DA INFORMAÇÃO

Trabalho de Conclusão de Curso apresentado como requisito para concessão do título de Bacharel em Direito pela Universidade Federal do Estado do Rio de Janeiro (UNIRIO), sob orientação do Prof. Dr. Leonardo Mattietto.

Rio de Janeiro

2018

“We’re able to view just everything that they do. And that’s really where data is going today. Data is the new oil.” - Bill Diggins

AGRADECIMENTOS

Agradeço de todo o coração à minha mãe, Maria Aparecida, por todo o apoio nesta jornada, sem o qual eu jamais teria conseguido chegar onde estou. Tudo o que faço é para orgulhá-la e ver um sorriso em seu rosto.

À minha irmã, Julia, que esteve comigo sempre que precisei, sempre acreditando mais em mim do que eu mesma.

Ao Frederico, meu melhor parceiro, pela paciência, interesse em meus trabalhos e pela compreensão mesmo nos momentos mais difíceis.

Aos meus amigos da turma 2013.2, em especial à Sarah, Jessica, Flora e Bruna, nossa eterna representante. Obrigada pelos momentos que compartilhamos e tarefas que executamos. Com vocês esta meia década de estudos foi ainda mais valiosa. O curso acaba, mas sei que seguiremos juntas na próxima fase de nossas jornadas.

Ao meu orientador, Leonardo Mattietto, pelos ensinamentos, disponibilidade e paciência na condução deste trabalho.

RESUMO

O presente trabalho tem como objetivo o estudo do direito fundamental à privacidade e sua relação com a proteção dos dados pessoais na sociedade da informação. No primeiro capítulo, faz-se uma breve análise da influência da evolução tecnológica e seu impacto na sociedade, e consequentemente no mundo jurídico. Realiza-se ainda a introdução de alguns conceitos relevantes para a perfeita compreensão do tema, como a evolução da concepção da privacidade e quanto aos diferentes tipos de dados que podem ser tratados, tendo em vista que nesta seara há uma estreita relação com nomenclaturas típicas da tecnologia da informação que normalmente não integram o cotidiano do profissional do direito. No segundo capítulo é feito o estudo das possíveis violações dos dados pessoais, as formas como isto pode ocorrer e suas potenciais consequências para os titulares dos dados. Neste tópico, é comentado ainda o famoso caso do escândalo do uso de dados de milhões de usuários do Facebook pela empresa Cambridge Analytica, que se tornou um marco histórico tendo repercussões inclusive políticas e financeiras de grande monta. No terceiro e último capítulo é feito um estudo das respostas às violações, analisando-se a regulamentação concernente ao tema, verificando o tratamento jurídico feito por alguns países, finalizando com uma análise do panorama da regulamentação nacional, suas perspectivas e influências. Conclui-se que a vida privada e a intimidade, direitos constitucionalmente previstos, para que tenham uma efetiva proteção no atual cenário, demandam uma regulamentação do uso dos dados pessoais, tendo em vista os potenciais efeitos danosos a seus titulares no caso de seu uso irresponsável.

.

Palavras-Chave: regulamentação da proteção de dados pessoais; tecnologia da informação, Regulamento Geral de Proteção de Dados (RGPD); violação dos dados pessoais.

ABSTRACT

This work aims to study the fundamental right to privacy and its relation to the protection of personal data in the information society. In the first chapter, a brief analysis is made of the influence of technological evolution and its impact on society, and consequently on the legal world. It also introduces some essential concepts, relevant to the correct understanding of the theme, such as the evolution of the concept of privacy and the different types of data that can be treated, considering that there can be used nomenclatures typical of the information technology field, that normally do not integrate the daily routine of the legal professional. The second chapter examines possible violations of personal data, the ways in which this may occur and the potential consequences for the individuals who may have their data used. In this topic, we also study the famous scandal that culminated in the unwarned use of data from millions of Facebook users by the company Cambridge Analytica, which has become a historical landmark having enormous political and financial repercussions. In the third and last chapter, it is made a study of the responses to violations that may occur, as seen before, analyzing the regulations concerning the subject, verifying the legal treatment made by some countries, ending with an analysis of the Brazilian regulation scenario, its perspectives and influences. Finally, it is inferred that private life and privacy, constitutionally foreseen rights, in order to have an effective protection in the current scenario, require a regulation of the use of personal data, given the potential harmful effects to the ones that have their data treated due to irresponsible use of it.

Key-words: data protection regulation; Information technology, General Data Protection Regulation (GDPR); violation of personal data.

SUMÁRIO

Introdução

Atualmente vivemos no que se convencionou a chamar de sociedade da informação, onde o fluxo de informações foi extremamente facilitado pelos avanços da tecnologia, em especial pelo advento da rede mundial de computadores, que permite a troca de um volume de dados sem precedentes.

Diante desta nova realidade, a própria sociedade sofreu alterações sensíveis, deixando algumas questões para trás, como por exemplo a dificuldade de comunicação a distância e sua demora, hoje em dia pessoas polos diametralmente opostos do mundo podem se comunicar praticamente de forma instantânea através da internet. Por outro lado, agora esta sociedade passa a ter que lidar com situações inéditas e eventuais novos problemas que podem demandar uma resposta jurídica, como é o caso do uso de dados pessoais, o que suscita novas questões quanto à privacidade.

No presente, o tratamento de dados pessoais tem sido uma questão altamente relevante e largamente discutida em muitos países, e inclusive já abordada no Brasil, ainda que de forma mais simples se comparada com a União Europeia ou mesmo outros países da américa latina. Isto se deve ao fato de que, com o enorme fluxo de informações que se tem contemporaneamente, é possível realizar o cruzamento de dados provenientes de diversas fontes a fim de criar previsões estratégicas quanto ao mercado, política e a vida pessoal dos titulares destes dados.

Os dados pessoais têm se mostrado um insumo cada vez mais valioso. Já há inclusive empresas, conhecidas como *data brokers*, que se especializam em coletar dados relevantes, organizá-los de modo que se possa extrair informações relevantes e depois os vendem para outros interessados, normalmente empresas, a fim de direcionar a publicidade, conhecer melhor o perfil dos clientes, definindo seu risco antes mesmo que eles contratem um seguro. Os próprios governos podem se beneficiar disto, adaptando suas políticas conforme resultados de pesquisas e outras informações obtidas a partir do cruzamento de dados.

Assim sendo, o presente trabalho pretende analisar o uso de dados, as possíveis violações e outras consequências que podem advir disto e quais as respostas jurídicas que podem ser dadas, a fim de regulamentar seu uso, protegendo a intimidade e a vida privada.

No primeiro capítulo é feita uma análise histórica da evolução da tecnologia e a influência disto na sociedade e consequentemente no direito, comentando inclusive as gerações de leis de proteção de dados que se seguiram. Neste capítulo, ainda, faz-se uma conceituação de alguns termos relevantes, relacionados com o campo da tecnologia da informação, que serão abordados ao longo deste estudo.

No segundo capítulo é feito um estudo das possíveis violações que podem ocorrer quanto ao uso de dados pessoais, seja na coleta, no processamento ou mesmo na difusão destes, e as possíveis consequências, tanto para o indivíduo titular dos dados quanto em grande escala, para uma massa de pessoas. Diante disto, comentamos o caso do uso de dados, não autorizado, de usuários do Facebook feito pela empresa Cambridge Analytica, que teve grandes repercussões em 2018.

No terceiro e último capítulo, faz-se uma análise do tratamento jurídico realizado por alguns países, com enfoque na regulamentação mais relevante para o tema, como é o caso do Regulamento Geral de Proteção de Dados da União Europeia, que passou a ter plena eficácia em 25 de maio de 2018, exercendo influência internacional neste tocante, visto que inclusive empresas que prestam bens e serviços para titulares de dados da União Europeia devem estar em compliance com o referido regulamento para poder continuar tratando os dados. Finalmente, abordamos o panorama jurídico brasileiro atual, quanto às suas previsões constitucionais e infraconstitucionais, além das propostas atuais de regulamentação do tema.

Por fim, é abordada a necessidade de regulamentação no Brasil diante das exigências internacionais e do próprio cenário interno, que demanda uma resposta jurídica atual e eficiente para com as situações que ocorrem hodiernamente.

1. Histórico e conceitos essenciais

1.1 A influência da evolução tecnológica no direito

O direito é uma construção social[1] em permanente fluxo histórico, moldado conforme as necessidades humanas que ao longo do tempo se modificam. A evolução tecnológica é um dos fatores mais relevantes nas relações sociais e consequentemente de essencial análise por parte do direito.

A humanidade continuou se modernizando e as inovações criaram novas situações inéditas na sociedade, alterando tanto a política, quanto a economia e as relações sociais de modo geral. A internet permitiu a derrubada de barreiras físicas e um fluxo de informação sem precedentes.

A evolução tecnológica sempre esteve acompanhada de novas abordagens do direito, afinal, este não pode ficar engessado diante das mudanças fáticas, sob pena de deixar de atender às demandas sociais, tornando-se obsoleto, ou mesmo ineficiente, simplesmente não abarcando as novas situações cotidianas. Diante disso, novos direitos e possíveis violações deles devem ser explorados a fim de proporcionar as garantias aos usuários.

> "That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society." [2]

Desde a década de 80, o mundo encontra-se no que se convencionou a chamar

---

[1] COELHO, Luiz Fernando. *Teoria Critica do Direito.*3ª Edição. Belo Horizonte. Del Rey, 2003. p. 277

[2] WARREN, Samuel; BRANDEIS, Louis. The right to privacy. *Harvard Law Review*, v. 4, n. 5. p. 193-220. 1890. Disponível em: < http://www.jstor.org/stable/pdf/1321160.pdf?refreqid=excelsior%3A8c00c00b2e2c0c87e1676989f6c46858> Acesso em 2018

de a “Era da Informação”[3], dados os grandes avanços da indústria da computação e sua crescente popularização. Esta “sociedade da informação”, expressão utilizada para os sucessores da “sociedade pós-industrial” e que pretende transmitir um novo paradigma socioeconômico, tem como insumo básico não mais apenas as fontes de energia, como foram o carvão e o petróleo, mas sim os ditos insumos de informação, propiciados pelas melhorias nas telecomunicações e microeletrônica[4].

> “A informação contém em si o principal ativo da sociedade da informação, ou seja, sua principal riqueza, sendo indispensável ao desempenho de qualquer atividade – o que explica a nomenclatura atribuída pela doutrina a essa nova forma de organização social, política e econômica. O trabalho, a educação, a saúde, o lazer, a política, a economia, enfim, tudo depende de informação. Após a supervalorização da terra na época da revolução agrícola e o predomínio dos bens de produção na revolução industrial, o que prepondera agora é a informação. Na qualidade de principal matéria-prima desse novo modelo capitalista, a informação se impõe como condição determinante para o desenvolvimento econômico e cultural da sociedade, daí o intensivo uso da tecnologia da informação – enquanto mecanismo facilitador da coleta, produção, processamento, transmissão e armazenamento – o que acarreta avassaladoras mudanças no mundo.[5]

Diante disto, novos instrumentos normativos vieram regulamentar as matérias que envolvem o uso de dados e a transmissão de informações, dando especial atenção à privacidade dos usuários. E com relação a isto, a Europa e os Estados Unidos foram pioneiros no tocante à legislação e inclusive jurisprudência acerca do tema da privacidade. A doutrina cita inclusive gerações destas normas voltadas à proteção de dados.[6]

A primeira geração teria surgido na década de 70, em resposta ao

---

[3] GERMAN, Christiano. *O caminho do Brasil rumo à era da informação.* Konrad-Adenauer-Stiftung. 2000. p.16.

[4] WERTHEIN, Jorge. A sociedade da informação e seus desafios. *Ciência da informação*, Brasília, v. 29, n. 2. p. 71-77. 2000.

[5] VIEIRA, Tatiana Malta. *O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação.* 2007.

[6] MENDES, Laura Schertel. *Privacidade, Proteção de Dados e Defesa do Consumidor.* Saraiva. p. 38-44. 2014.

processamento eletrônico feito pelo poder público e por empresas privadas, em razão da criação de bancos de dados. O contexto do Estado do Bem-Estar Social, sob o argumento de buscar um planejamento que melhor atendesse às peculiaridades de sua população local, passou a realizar o tratamento de dados a fim de cruzar informações que viabilizassem um melhor reconhecimento estatístico da sociedade, identificando assim padrões, tendências, preferências e afins.[7]

Nos EUA, por exemplo, sob o argumento de reduzir os custos, houve inclusive uma tentativa de criação do "National Data Center", um banco de dados que centralizaria todos os dados dos cidadãos americanos; registros de trabalho, censo, recolhimento de impostos e até mesmo sobre o seguro social. Eventualmente outras fontes de informação ainda seriam adicionadas.[8]

Seguiram-se então inúmeras discussões quanto à criação do banco de dados, especialmente quanto aos possíveis danos que tamanha centralização poderia causar. Foi publicado um artigo na New York Times Magazine, *"Don't Tell It to the Computer"* do autor Vance Packard, que também publicou o livro "*The Naked Society",* atacava a ideia de uma centralização nas mãos do governo, denunciando a invasão da privacidade por parte do governo. Seus argumentos foram valiosos contra o projeto, que não chegou a se concretizar.

A opinião pública, à época, optou por controlar a tecnologia e o funcionamento dos bancos de dados, ante o receio diante da crescente capacidade de processamento de dados e seus possíveis desdobramentos. Isso foi refletido na primeira geração de normas de proteção de dados, que buscaram regulamentar esses centros, tornando necessária a autorização para sua criação e posteriormente o controle deles por órgãos públicos. Como exemplos, podemos citar a Lei do Land Hesse de 1970 (Alemanha), Estatuto Para Bancos de Dados de 1973 (Suécia) e o

---

[7] MENDES, Laura Schertel. *Privacidade, Proteção de Dados e Defesa do Consumidor.* Saraiva. p. 38-39. 2014.

[8] GARFINKEL, Simson. *Database nation: the death of privacy in the 21st century.* O'Reilly Media, Inc. p. 13. 2000.

Privacy Act de 1974 (EUA)[9].

Porém, ante a constante modernização da tecnologia, algumas dessas leis passaram a ficar ultrapassadas. A capacidade cada vez maior de processamento de dados tonou o sistema de autorizações e fiscalização detalhada mais dificultoso, vez que o fluxo de dados se tornou cada vez maior, prejudicando essa análise por um crivo mais minucioso.

Isto deu ensejo a uma segunda geração de normas voltadas à proteção da privacidade dos dados pessoais, com características estruturalmente diferentes. Focava-se agora no direito à privacidade como uma liberdade negativa do indivíduo, e como exemplo disto temos a lei francesa *Informatique et Libertés*[10]*,* em alguns países como Áustria, Espanha e Portugal a privacidade informacional inclusive foi inserida nos textos constitucionais[11].

Em lugar de uma tentativa de controle extenso do Estado sobre a intimidade de seus cidadãos, essa nova geração de leis pretendia garantir maior proteção à privacidade e ao mesmo tempo uma intervenção mínima na esfera pessoal, garantindo maior liberdade e "o direito de ser deixado só".

No entanto, estas leis também se mostraram insuficientes. O fornecimento de dados pessoais por parte dos usuários tornara-se condição necessária para o uso de diversos recursos oferecidos, pelo Estado e especialmente por empresas, e consequentemente um requisito para a interação social e participação na sociedade gradualmente mais digital, vez que para o uso das ferramentas de informática requer-se um cadastramento do usuário.[12]

---

[9] PASSOS, Bruno Ricardo dos Santos. *O direito à privacidade e a proteção aos dados pessoais na sociedade da informação: uma abordagem acerca de um novo direito fundamental.* p. 55-57. 2017.

[10] PASSOS, Bruno Ricardo dos Santos. *O direito à privacidade e a proteção aos dados pessoais na sociedade da informação: uma abordagem acerca de um novo direito fundamental.* p. 55-57. 2017.

[11] MENDES, Laura Schertel*. Privacidade, Proteção de Dados e Defesa do Consumidor.* Saraiva. p. 40. 2014.

[12] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar. p. 210.

Diante disto, ainda na década de 80 surge uma terceira geração de leis. Nesta fase busca-se ampliar a proteção à medida que o indivíduo não apenas tem a opção de fornecer ou não seus dados, a lei agora busca a maior efetividade da proteção à privacidade. Em famosa decisão, o Tribunal Constitucional Alemão, em 1983, declarou que os cidadãos têm direito à autodeterminação informativa, conferindo ao cidadão maior poder de participação em todo o processo de tratamento de seus dados, garantindo-lhes maior conhecimento sobre as operações pelas quais passam essas possíveis informações sobre si[13].

No entanto, o ideal participativo dos cidadãos, a autodeterminação informativa *per se,* provou-se impraticável dado que, assim como na segunda geração, cada vez mais os usuários tornaram-se dependentes das tecnologias no dia a dia. Para participar minimamente da sociedade da informação, especialmente em centros urbanos, nos polos mais desenvolvidos, os cidadãos estavam cada vez mais dispostos a ceder seus dados em troca de serviços e benefícios que poderiam ser oferecidos, muitas vezes aderindo aos termos de uso sem ao menos ler suas previsões, consentindo assim quanto ao uso dos seus dados, dificultando eventual reparação em razão da violação de sua privacidade, tendo em vista a autorização do uso destas informações.

Por fim, desenvolveu-se uma quarta geração de normas relativas à proteção de dados pessoais, buscando trazer soluções para os problemas anteriormente experimentados, tentando tornar mais efetivo o controle dos indivíduos sobre seus dados e inclusive passando a considerar alguns temas relativos aos dados pessoais tão preciosos que merecem ser superprotegidos, considerados como um verdadeiro direito fundamental indisponível, a fim de resguardar os indivíduos. A exemplo disso, a doutrina de Laura Schertel Mendes cita os dados sensíveis, relativos ao credo, opção sexual, histórico médico e outros dados cujo tratamento tem o potencial de

---

2006.

[13] MENDES, Laura Schertel. *Privacidade, Proteção de Dados e Defesa do Consumidor.* Saraiva. p. 41-42. 2014.

gerar discriminação, acarretando prejuízos à pessoa da qual provém.[14]

Atualmente, na União Europeia a proteção dos dados já é tida como um direito fundamental, vide o art. 8º da Carta dos Direitos Fundamentais da União Europeia, instrumento juridicamente vinculativo nas instituições e órgãos da União e dos estados membros. A quarta geração destas normas de proteção tem como característica a criação de normas gerais, mais abrangentes e flexíveis, que servem como diretrizes para normas setorizadas, e que melhor se adequem à realidade local. A Diretiva 95/46/CE do parlamento europeu foi um marco neste sentido, estabelecendo princípios e direitos que serviriam de base para legislações suplementares nos países membros, e também serviria como inspiração para outras nações.

O Brasil também teve influências estrangeiras no campo da proteção dos dados pessoais. Há previsões de proteção à privacidade e aos dados pessoais no Marco Civil, porém ainda de forma simples, a ser regulamentada. Diante desta previsão e da evidente necessidade de regulamentação, há projetos de lei em andamento que pretendem a regulamentação da proteção dos dados pessoais em território nacional, como o PL 4060/2012, o PLS 330/2013 e o PL 5276/2016, que serão abordados em outro momento.

> "A rápida evolução tecnológica e a globalização criaram novos desafios em matéria de proteção de dados pessoais. A recolha e a partilha de dados pessoais registaram um aumento significativo. As novas tecnologias permitem às empresas privadas e às entidades públicas a utilização de dados pessoais numa escala sem precedentes no exercício das suas atividades. As pessoas singulares disponibilizam cada vez mais as suas informações pessoais de uma forma pública e global. As novas tecnologias transformaram a economia e a vida social e deverão contribuir para facilitar a livre circulação de dados pessoais na União e a sua transferência para países terceiros e organizações internacionais, assegurando simultaneamente um elevado nível de proteção dos dados pessoais. "[15]

---

[14] MENDES, Laura Schertel. *Privacidade, Proteção de Dados e Defesa do Consumidor.* Saraiva. p. 43. 2014.

[15] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. Disponível em: http://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em 2018.

Assim, sendo verificada a influência da tecnologia na sociedade através da história, e consequentemente no direito, passar-se-á primeiramente à conceituação de alguns tópicos a fim de possibilitar a melhor compreensão do tema.

1.2 Privacidade

O conceito de privacidade alterou-se ao longo do tempo, estando presente nas mais diversas sociedades. Sua concepção moderna, porém, identificada pela doutrina da *common law* no pioneiro artigo "*The right to privacy"*[16]*,* afigurava-se exacerbadamente individualista. Buscando assegurar "o direito de ser deixado só", como foi assim chamado pelo Juiz Cooley, a visão da privacidade era um direito negativo, esperava-se que o Estado se abstivesse de qualquer intromissão na esfera privada, herança de uma tradição burguesa[17].

> "Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone."

Os autores revolucionaram o conceito na medida em que passaram a relacionar o direito à privacidade com a inviolabilidade da personalidade em lugar da proteção à mera propriedade privada[18]. A proteção seria então uma garantia, não dos bens que a pessoa possuía, mas sim uma proteção da pessoa em si.

Buscava-se um instrumento jurídico capaz de proteger a esfera da vida privada, inicialmente voltando-se mais para casos de personalidades famosas, cuja vida privada era constantemente invadida por jornalistas, por exemplo, já dotados de novas tecnologias como as recém-criadas máquinas de fotografia.

---

[16] WARREN, Samuel; BRANDEIS, Louis. The right to privacy. *Harvard Law Review,* v. 4, n. 5. p. 193-220. 1890.

[17] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar. p. 5. 2006.

[18] MENDES, Laura Schertel. *Privacidade, Proteção de Dados e Defesa do Consumidor.* Saraiva. p. 28. 2014.

Desde então a doutrina ainda evoluiu, reinventando o significado do direito à privacidade, bem como sua extensão. De um direito individualista, "fechado", aos poucos ele se transformou em uma garantia de controle do indivíduo sobre as próprias informações, cuja complexidade vai além do mero isolamento social, tornando-se verdadeiro pressuposto para um regime democrático[19]. Ensina Danilo Doneda que a introdução do modelo w*elfare state,* alterando a relação do cidadão com o Estado, tendo este adotado um cunho mais assistencialista e buscando garantir um patamar mínimo de bem-estar social geral, juntamente com um maior fluxo de informações em razão dos avanços tecnológicos, contribuíram para uma inflexão da tendência anterior.

> "...nos últimos dez anos, o assunto da privacidade ganhou novas facetas, em virtude da disseminação das tecnologias de tratamento da informação. São essencialmente três os fenômenos que vêm contribuindo para uma maior preocupação com o tema: primeiramente, a estruturação de bases de dados, que abriu a possibilidade de se cruzar informações com grande facilidade, construindo perfis detalhados de praticamente qualquer pessoa, a um custo baixo, até mesmo sem a ciência do interessado; em segundo lugar, a disseminação da informática, que culminou com a ampla utilização da Internet, estimulando praticamente a todos a manterem em forma digital as suas informações, facilitando a sua coleta; e, finalmente, a padronização de equipamentos e sistemas, o que facilitou a aquisição de informações mantidas por usuários de informática, inclusive sem o seu conhecimento."[20]

Diante desta nova estrutura, tonou-se essencial rediscutir as definições e limites da privacidade, bem como sua extensão, de que forma deve ser resguardada, e ainda qual a responsabilidade daqueles que tratam dos dados pessoais, sejam estes o Estado ou, como tem sido mais comum, empresas.

Atualmente, o grande volume de circulação de dados a fim de obter informações precisas acerca dos gostos de seus clientes tem se tornado uma prática comercial cada vez mais comum. Saber o que o cliente quer, com base em seu perfil

---

[19] MENDES, Laura Schertel. *Privacidade, Proteção de Dados e Defesa do Consumidor.* Saraiva. p. 28. 2014.

[20] LINS, Bernardo F. E. Privacidade e internet. *Estudo técnico da Consultoria Legislativa.* p.3. Brasília: Câmara dos Deputados/Consultoria Legislativa. 2000.

pode significar uma grande vantagem sobre seus concorrentes, aumentando as chances do seu produto ser escolhido, por exemplo.

Nos Estados Unidos e na União Europeia, a discussão acerca da privacidade no mundo digital já se encontra mais amadurecida, resultando em leis e diretrizes que tem como objetivo regulamentar a matéria e prevenir abusos.

Neste contexto em que a tecnologia permite o maior processamento de dados pessoais, possibilitando diversos usos, a privacidade tem que ser associada à proteção destas informações. Com isto o próprio conteúdo deste direito fundamental tem sido alterado, inclusive quanto ao seu léxico, passando a ser reconhecido em diversos países, como uma verdadeira projeção da personalidade do indivíduo, merecendo tutela jurídica, e inclusive com status constitucional, como é o caso da Espanha, Portugal, Hungria, Eslovênia e Rússia.[21]

1.3 Dados pessoais

O conceito jurídico de “dado” diverge de “informação” na medida em que aquele pode ser considerado um precursor de uma informação, símbolos e sinais que, quando interpretados competentemente, se convertem em conhecimento. Assim sendo, o “dado” precisa ser repassado e compreendido pelo receptor para que que se transforme, de forma inteligível, em uma informação[22].

Os dados pessoais, por sua vez, são assim definidos no art. 4º do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, que diz respeito à proteção das pessoas, o tratamento de dados pessoais e à livre circulação desses dados.

---

[21] MENDES, Laura Schertel. *Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo.* p. 18. 2010. Disponível em: < http://www.repositorio.unb.br/bitstream/10482/4782/1/DISSERTACAO%20LAURA.pdf> Acesso em 2017.

[22] WACKS, Raymond. Personal information: privacy and the law. *Oxford: Clarendon Press.* 1989.

> "«Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;"[23]

A informação pessoal, por sua vez, possui um vínculo objetivo com a pessoa da qual advém, podendo revelar seus aspectos íntimos. Podem ser fatos, opiniões e afins que o indivíduo prefira guardar para si, ou mesmo limitar a circulação desta informação a fim de se resguardar. Diante da constatação de que tais informações constituem atributo da personalidade e dizem respeito, portanto, à própria pessoa, entende a doutrina que estes dados merecem tutela jurídica[24].

Na Europa, pioneira no aspecto da proteção dos dados pessoais, a proteção das pessoas singulares relativamente ao tratamento de seus dados já é um direito fundamental, vide o artigo 8, nº 1, da Carta dos Direitos Fundamentais da União Europeia e o artigo 16, nº 1, do Tratado sobre o Funcionamento da União Europeia (TFUE).

No Brasil, porém, ainda estão pendentes de maior regulamentação os mecanismos de proteção aos dados pessoais. Não obstante, a Constituição Federal põe a salvo a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, incluindo-os no rol dos direitos fundamentais sendo estes desde já autoaplicáveis.

O Marco Civil da Internet, Lei 12.965/2014, lei com maior enfoque nos dados eletrônicos, define como seus princípios, em seu art. 3º, as seguintes diretrizes.

---

[23] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. Art. 4, 1. Disponível em: http://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em 2018

[24] MENDES, Laura Schertel. *Privacidade, Proteção de Dados e Defesa do Consumidor.* Saraiva. p. 56-57. 2014.

"Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
II - proteção da privacidade;
III - proteção dos dados pessoais, na forma da lei;"[25]

No mais, há projetos de lei com a finalidade de realizar esta regulamentação, atualmente tramitando, e que serão abordados no presente trabalho.

1.4 Dados anônimos

Por definição, são anônimos aqueles que preservam a identidade daqueles de quem a informação advém. Referindo-se a pessoas indeterminadas, os dados anônimos podem ser então utilizados para fins estatísticos, comumente utilizados para censos, por exemplo. [26]

Quando os dados coletados são tratados de modo a impossibilitar a identificação de sua origem, a eles não são aplicáveis os princípios protetivos adotados quantos aos dados pessoais, tendo em vista que sem a identificação da pessoa, sua intimidade permanece resguardada.

1.5 Dados sensíveis

Dados sensíveis, por sua vez são informações que necessitam de proteção especial, tendo em vista seu potencial discriminatório, ou seja, o conhecimento dessas informações pode vir a gerar prejuízo para as pessoas, ou mesmo organizações, a quem dizem respeito.[27]

---

[25] BRASIL. Marco Civil da Internet, Lei 12.965/2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>

[26] MENDES, Laura Schertel. *Privacidade, Proteção de Dados e Defesa do Consumidor.* Saraiva. p. 56-57. 2014.

[27] WENDT, Emerson; FREITAS, Lidiane Marques; CALHEIROS, Tânia da Costa. *Dados Sensíveis: uma análise do Art. 5º, Inciso III, do PL nº 5276/2016 para a proteção de dados pessoais*. 2017. Disponível em: < http://direitoeti.com.br/site/wp-content/uploads/2017/10/WENDT-FREITAS-

O projeto de lei 5276/2016, da Câmara dos Deputados, que pretende conferir aos dados sensíveis proteção especial, os conceitua da seguinte forma.

> "III – dados sensíveis: dados pessoais que revelem a origem racial ou étnica, as convicções religiosas, filosóficas ou morais, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual e dados genéticos ou biométricos."

Na Europa estes dados já gozam de proteção diferenciada, tendo especial atenção, estando seu tratamento condicionado ao consenso expresso e informado do indivíduo, sendo inclusive possível aos cidadãos proibir o uso destes dados pessoais para fins de marketing direto.[28]

1.6 Tratamento e refinamento

O tratamento de dados pode ser definido da seguinte forma:

> "«Tratamento», uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição; "[29]

Assim sendo, tem-se que o tratamento é um procedimento, informatizado ou não, operado nos dados obtidos a fim de deles extrair a informação útil. É a partir

---

CALHEIROS_Dados-Sens%C3%ADveis.pdf> Acesso em 2018.

[28] MENDES, Laura Schertel. *Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo.* 2010. p. 39 Disponível em: < http://www.repositorio.unb.br/bitstream/10482/4782/1/DISSERTACAO%20LAURA.pdf> Acesso em 2017

[29] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. Art. 4, 2. Disponível em: http://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em 2018

deste processamento que é possível a definição de perfis, que consiste numa avaliação dos aspectos pessoais da pessoa que teve seus dados tratados, a fim de prever aspectos de sua vida privada, tais quais seu desempenho profissional, situação econômica, saúde, preferências, comportamento e afins.[30]

A doutrina costuma se ater a três etapas específicas deste tratamento, as que podem acarretar mais riscos à personalidade e que consequentemente são o foco do presente estudo, e objeto de tutela jurídica, são elas; a coleta, processamento e difusão, que serão aprofundados ao tratar das violações e legitimidades. [31]

[30] Diretiva UE 2016/680. Art 3º, 3.

[31] MENDES, Laura Schertel. *Privacidade, Proteção de Dados e Defesa do Consumidor.* Saraiva. p. 94-95. 2014.

2. A violação dos dados pessoais

Neste tópico, pretende-se discorrer sobre as possíveis formas de violação dos dados pessoais, da própria privacidade, mostrando alguns dos métodos atuais utilizados tanto para a coleta quanto para o tratamento ou a difusão de dados e suas implicações.

Nesta sociedade da informação, que progressivamente está se tornando progressivamente mais "*smart*", o estilo de vida progressivamente mais tecnológico representa um desafio crescente à proteção da privacidade. Muitos dos titulares de dados, normalmente consumidores de produtos e serviços, não estão a par das implicações do uso de seus dados, e acabam por trocar de bom grado sua privacidade a fim de manter seu modo de vida moderno.[32]

Nas mídias sociais, cada vez mais as pessoas compartilham suas informações, sejam suas fotos do dia a dia, seus registros de acontecimentos importantes ou mesmo simples interações com os contatos, dessa forma elas estão a gerar enormes quantidades de dados. Inclusive em casa, especialmente com a chegada do conceito de "internet das coisas" onde os aparelhos do cotidiano estariam todos ligados à internet, desde a geladeira à televisão, todos com uma capacidade crescente de coletar os dados dos seus usuários sob o pretexto de oferecer um serviço melhor, mais personalizado e prático.

Atualmente fala-se muito do *Big Data,* que consiste em um grande volume de dados que são submetidos a um conjunto de soluções tecnológicas, sendo assim possível analisar estes dados em velocidades muito superiores à capacidade de processamento de um ser humano.[33] É como um microscópio, grosso modo comparando, a partir de novos recursos decorrentes dos avanços da tecnologia, a capacidade de examinar o espectro da sociedade se tornou muito maior.

---

[32] PEISSL, Walter; KRIEGER-LAMINA, Jaro. *The scored consumer: privacy and big data. In: International Conference on Consumer Research (ICCR)*, DEU. p. 105. 2017.

[33] PINHEIRO, Patrícia Peck. Direito digital. Saraiva. p. 96. 2016.

Neste contexto ocorre o tratamento de dados, que compreende estas operações que podem ser realizadas sobre estes fragmentos para refiná-los e extrair mais informações. A doutrina indica três momentos específicos deste tratamento que podem acarretar maiores risco à personalidade, sendo eles: coleta, processamento e difusão.[34]

A coleta é a fase de obtenção das informações, direta ou indiretamente. Afinal, há diversas formas de angariar informações, como na criação de cadastros de consumidores, em pesquisas de mercado, sorteios e mesmo através de aplicativos. Exemplo desta coleta foi o caso da Cambridge Analytica, que será abordado com maior profundidade em tópico próprio, onde as pessoas que instalavam o aplicativo acabavam por fornecer acesso até mesmo aos dados de seus amigos quando faziam uso do aplicativo.

O processamento é a fase de lapidação dos dados, onde estes são submetidos a algumas técnicas a fim de extrair informações relevantes. A mineração de dados é um exemplo, onde por meio da combinação dos dados e de recursos estatísticos insumos informativos valiosos podem ser extraídos dos dados coletados. Há ainda outras técnicas, como o *profiling* e o *scoring,* que serão tratados no presente capítulo.

Por fim, na difusão, a fase de uso em definitivo, que compreende inclusive a possibilidade de transferência destes dados a terceiros, está intrinsecamente ligada ao princípio da finalidade, segundo o qual a finalidade do tratamento deve ser informada ao titular, e ele deve ter o poder de optar por fornecê-los para aquela finalidade específica, garantindo a legitimidade do tratamento. Havendo desvio de sua finalidade, se os dados são difundidos de forma diferente do acordado, ocorre uma quebra na relação de confiança, acarretando uma perigosa violação.

A violação dos dados é assim definida pelo Regulamento Geral de Proteção de

---

[34] MENDES, Laura Schertel. *Privacidade, Proteção de Dados e Defesa do Consumidor*. Saraiva. p. 94-95. 2014.

Dados da UE:

> “12) «Violação de dados pessoais», uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento;”

Em especial na internet, as violações à privacidade podem acontecer de diversas formas. Seja de modo análogo à imprensa, com a divulgação aberta de dados pessoas, ou de forma velada, com o recolhimento e análise destes a fim de obter informações para fins diversos, especialmente quando não há consentimento informado do usuário.

Verifica-se, portanto, a necessidade de um consentimento informado do titular dos dados, é necessário que ele seja notificado de que seus dados estão sendo coletados, que serão usados e para qual finalidade a fim de que seja legítimo o tratamento.

A seguir, passar-se-á a discorrer sobre algumas técnicas de tratamento de dados, seu alcance e eficiência além de seus possíveis riscos, casos de violação da privacidade.

2.1. Formas possíveis violação da privacidade

No atual contexto da sociedade da informação, qualquer pessoa é capaz de gerar dados, e estes podem reproduzir as mais diversas informações, especialmente sobre a esfera da vida privada. Estas informações obtidas a partir do tratamento desses dados, muitas vezes coletados sem um consentimento verdadeiramente informado do indivíduo, são frequentemente utilizadas para fins lucrativos, podendo ser vendidas a terceiros ou mesmo utilizadas pelos próprios responsáveis pelo tratamento a fim de obter uma vantagem competitiva, o que pode ensejar verdadeiras violações aos direitos da personalidade.

> "Ocorre que, muitas vezes, os cidadãos e especialmente os usuários das novas ferramentas tecnológicas como a internet, têm sua privacidade e intimidade violadas por pessoas físicas ou jurídicas que buscam obter suas informações a todo o custo. Além disso, uma vez armazenada a informação, ela é repassada a terceiros sem o consentimento – ou, pior, sem o conhecimento – dos titulares dos dados. Configura-se, daí uma verdadeira violação ao direito à privacidade dos indivíduos, que ficam à mercê de quem detém o conhecimento técnico, sem poder ter controle das informações sobre si mesmo, as quais são bens privados de cada um e merecem a devida proteção e respeito. Porém, no que diz respeito ao titular desses dados, muitas vezes a apropriação de tais informações por terceiros gera constrangimento e/ou revolta, por se tratarem de dados privados. "[35]

O crescente desenvolvimento da tecnologia tem possibilitado um tratamento cada vez mais eficiente dos dados. Atualmente empresas podem coletar e analisar um volume significantemente maior destes, com especial destaque para os dados obtidos na internet.

Estudos comprovam que, com base nos rastros digitais deixados pelos usuários na internet, muitas características e atributos destas pessoas podem ser previstos com base em seu comportamento digital. Meros "likes" no Facebook e outros *logs* de atividade permitem extrair, com grande precisão, informações pessoais altamente sensíveis, como a opção sexual, etnia, religião, posicionamento político, estado emocional, se a pessoa faz uso de substâncias que causam dependência, e até mesmo o estado gravídico de uma pessoa, antes dela mesma.[36]

Foi feita uma pesquisa com mais de 58.000 voluntários que forneceram seus dados quanto aos *"likes*" no Facebook, perfis demográficos detalhados e os resultados de testes psicométricos, que foram usados para fins de análise e comparação destes perfis com as predições a serem extraídas do tratamento feito

---

[35] MENDONÇA, Fernanda Graebin. Proteção de Dados Pessoais na Internet: Análises Comparativas da Situação do Direito à Autodeterminação Informativa no Brasil e Em Países Latino-Americanos. *Revista Jurídica da Faculdade de Direito de Santa Maria-FADISMA, v. 11, n. 1.* p. 283-311. 2016.

[36] KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences, v. 110, n. 15.* p. 5802-5805. 2013.

com base nos registros obtidos do Facebook. Os ditos "*likes*" são tidos como uma classe genérica de registros digitais comparáveis ao histórico de compras de cartões e históricos de internet. Diferentemente destes outros, porém, os registros feitos desta forma no Facebook são públicos, por padrão, possibilitando seu acesso e consequente uso por uma gama maior de interessados. O estudo conduzido buscou mostrar o quão precisas e potencialmente invasivas são as análises feitas a partir destes dados coletados, conforme é dito no artigo, vide transcrição abaixo.[37]

> "We distinguish between data that are actually recorded and information that can be statistically predicted from such records. People may choose not to reveal certain pieces of information about their lives, such as their sexual orientation or age, and yet this information might be predicted in a statistical sense from other aspects of their lives that they do reveal."

Neste estudo, feito de modo a identificar atributos e traços da personalidade, a taxa de sucesso quanto à classificação rendeu resultados impressionantes. A etnia, entre caucasianos e afro descentes, foi corretamente classificada em 95% dos casos. O sexo dos voluntários foi identificado em 93% dos casos, sugerindo um padrão de comportamento significantemente diferente entre os grupos, permitindo uma identificação quase perfeita. A religião, se cristão ou mulçumano, obteve uma taxa de acerto de 82%, e um resultado similar foi obtido quando à posição política dos sujeitos analisados, se Democrata ou Republicano, com uma taxa de 85%. E mesmo a orientação sexual foi possível de ser prevista com uma alta porcentagem de sucesso, entre os homens com uma taxa de 88% e entre as mulheres em 75% dos casos, sugerindo um comportamento online mais distinto entre os homens heterossexuais e homossexuais comparativamente.

Verifica-se, portanto, que é possível identificar diversos outros atributos pessoais a partir do tratamento de dados, que podem ser coletados de diversas formas e a partir de vários meios. Tais predições quanto a preferências e atributos podem ajudar a melhorar produtos e serviços, mas por outro lado eles também

---

[37] KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences, v. 110, n. 15.* p. 5802-5805. 2013.

podem ter implicações consideravelmente negativas, visto que são facilmente aplicáveis a grandes grupos de pessoas sem a obtenção de seu consentimento ou mesmo sem que eles estejam cientes. Isto pode ensejar violações à privacidade e mesmo a outros direitos da personalidade, por exemplo, ao revelar a gravidez de uma mulher não casada, através de vários anúncios e envios de vouchers quanto a produtos relacionados à maternidade, em uma cultura onde isto não seja aceito. Neste caso, tanto a liberdade quanto a própria vida da gestante podem estar ameaçadas.

Em um caso que ficou relativamente famoso, a Target, uma loja de departamento que oferece ampla gama de produtos, objetivando fidelizar os clientes, passou a investir em análise estatística dos dados de seus clientes para identificar perfis de compra, a fim de encaminhar cupons de desconto para os consumidores quanto a produtos que estivessem em categorias de seu interesse. Assim sendo, a empresa chegou a um rol de 25 itens que, quando comprados em conjunto indicavam que a consumidora possivelmente estava grávida, desta forma podendo desde logo encaminhar promoções a estas futuras mães, com isto aproximando-as da loja durante todo o período, ajustado as ofertas conforme as necessidades comuns.

Tal formula, porém, teria sido tão efetiva a ponto de inclusive expor a gravidez de uma adolescente antes mesmo que sua família soubesse.[38] Uma vez identificados os padrões de uma possível grávida, a loja começou a enviar os cupons de desconto de produtos de maternidade para o e-mail de uma adolescente, como era o padrão. O pai da menina, teria inclusive ido até a loja reclamar das propagandas que a filha estava recebendo. Pouco tempo depois, porém, a gravidez veio a ser confirmada.

O caso elencado ilustra com assustadora precisão a capacidade de

[38] LUBIN,Gus. The incredible story of how Target exposed a teen girl's pregnancy. *Business Insider*. 2012. Disponível em: https://www.businessinsider.com.au/the-incredible-story-of-how-target-exposed-a-teen-girls-pregnancy-2012-2. Acesso em 20/04/2018

profiling[39], a construção de perfis com base no cruzamento dos dados angariados, a fim de prever padrões de comportamento, preferência, hábitos e outras informações potencialmente relevantes. Como se percebe, muitos dados estão disponíveis, e são capazes de gerar informações importantes a partir de sua análise, podendo suportar decisões estratégicas decisivas e contribuindo para gerar recursos de inteligência e valor para empresas.

Por esta razão os dados pessoais têm sido comparados ao petróleo como insumo essencial desta geração. Eles podem ser cruzados a fim de obter maiores informações, em geral criando perfis de consumo[40]. Tais perfis são valiosos para empresas em geral que pretendem otimizar suas vendas. Sabendo as preferências dos consumidores, os anúncios tendem a ser mais eficientes, e consequentemente as vendas, tendo em vista que as ofertas passam a ser direcionadas para aqueles que tem as maiores chances de se interessar pelos produtos ofertados.

A partir desta construção de perfis, empresas podem realizar o *retargeting*, ou de forma mais específica, *remarketing*[41]. Isto consiste em encaminhar aos clientes anúncios personalizados, voltados para seus interesses pessoais de acordo com os dados obtidos a partir de suas pesquisas online, dos rastros digitais deixados, o que é considerado por muitos algo assustador, tendo em vista que ao consultar um produto em determinado site, um *vade mecum* por exemplo, este irá reaparecer em diversos sites através de anúncios ou mesmo em na caixa de e-mail, normalmente com indicação de itens relacionados, eventualmente até mesmo "denunciando" as pesquisas do usuário e promovendo um verdadeiro assédio de consumo[42].

---

[39] MENDES, Laura Schertel. *Privacidade, Proteção de Dados e Defesa do Consumidor*. Saraiva. p. 111-112. 2014.

[40] PASSOS, Bruno Ricardo dos Santos. *O direito à privacidade e a proteção aos dados pessoais na sociedade da informação: uma abordagem acerca de um novo direito fundamental.* p. 39. 2017.

[41] HELFT, Miguel; VEGA, Tanzina. Retargeting ads follow surfers to other sites. *The New York Times.* p. 8-11. 2010.

[42] DA SILVA GUESSO, Bruna de Oliveira et al. *O comércio eletrônico e o direito fundamental de defesa do consumidor.* 2018

A partir destes perfis de consumo torna-se viável fazer o *scoring* dos usuários, atribuindo um “valor” aos titulares dos dados, identificando por exemplo os “melhores consumidores”, os de menor risco a fim de fidelizá-los e oferecendo assim as melhores ofertas, por outro lado, também classificando os “piores consumidores”, considerando inclusive o grau de inadimplência, e estes uma vez classificados podem até mesmo não mais receber ofertas ou mesmo ter seu acesso a bens e serviços negados, gerando uma verdadeira discriminação em nome da otimização da administração do negócio.[43]

É possível ir além quanto a isto. Uma farmácia, por exemplo, ao vincular o CPF do comprador à sua respectiva lista de compras é capaz de angariar subsídios para criar um perfil com dados sensíveis que dizem respeito à saúde destes consumidores, o que eventualmente pode ser utilizado para realizar um *scoring* potencialmente perigoso. O uso de determinados produtos poderia indicar uma condição clínica ou mesmo a tendência a alguma doença, podendo ensejar discriminação do titular destes dados, por exemplo, na contratação de um seguro, de um plano de saúde ou até mesmo quanto à manutenção ou obtenção de um emprego.

É relevante apontar ainda que estes perfis, os cadastros em geral, podem conter erros, e estas falhas são capazes de gerar grandes prejuízos aos titulares dos dados. Ao classificar uma pessoa em uma categoria errada, como um consumidor inadimplente, a título de exemplo, este pode ter problemas para contratar e usufruir de bens e serviços, como já mencionado. Por esta razão, para que estes recursos, especialmente o *scoring,* tenham legitimidade, nas palavras de Laura Schertel Mendes, a transparência é um fator fundamental. Deve ser disponibilizado o acesso às informações do titular constantes no banco de dados, bem como os critérios objetivos usados para categorizar os titulares dos dados, além de dever ser oferecida a da possibilidade de retificação das informações.

---

[43] MENDES, Laura Schertel*. Privacidade, Proteção de Dados e Defesa do Consumidor.* Saraiva. p. 112-116. 2014.

Não apenas a doutrina, mas também os tribunais já estão tendo que se debruçar sobre o tema da proteção de dados, especialmente diante da informatização e do irrefreável avanço da internet, reconhecendo a capacidade de uso das informações extraídas para fins ilícitos e potencialmente lesivos aos direitos da personalidade, vide a seguinte transcrição de trecho do acórdão do STJ.

> "1. A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, 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. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos e privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica. A importância do tema cresce de ponto quando se observa o número imenso de atos da vida humana praticados através da mídia eletrônica ou registrados nos disquetes de computador. "[44]

Fica assim demonstrada a vulnerabilidade dos titulares dos dados, normalmente simples consumidores, diante das novas práticas do mercado, e a imprescindibilidade de acompanhamento das novas tendências por parte dos profissionais do direito, visto que as violações aos direitos da personalidade podem acontecer de diversas formas e a qualquer momento, conforme demonstrado. Mais que isto, é preciso que haja uma regulamentação adequada acerca da matéria, como já se tem avançado em alguns lugares, a exemplo da própria União Europeia, a fim de criar previsões de resposta e prevenção para casos como os comentados supra.

A seguir, passar-se-á a discorrer sobre um caso de violação de dados trazido à tona em 2018, que merece atenção especial dado o grande impacto sobre milhões de pessoas, sobre a economia e inclusive a política.

---

[44] STJ, Recurso Especial n. 22.337/RS, rel. Ministro Ruy Rosado de Aguiar, DJ 20/03/1995, p. 6119.

2.2. Caso Cambridge Analytica e Facebook

Recentemente teve grande repercussão o caso do vazamento e uso não autorizado dos dados de 87 milhões de usuários do Facebook. Isto se deu após seu ex-diretor de Tecnologia, Christopher Wylie, ir à imprensa e divulgar que os dados e milhares de usuários do Facebook haviam sido tratados por terceiros sem o seu consentimento. A responsável por isto foi a empresa Cambridge Analytica, pivô da questão, que realizava o tratamento de dados a fim de auxiliar seus clientes a obterem vantagens políticas e comerciais com base nas informações extraídas dessas operações.

A empresa vendia a ideia de uma aproximação mais efetiva tanto dos consumidores quanto dos eleitores, por parte dos contratantes, ao analisar os dados daqueles e poder oferecer um serviço mais personalizado e efetivo, conhecendo melhor o cliente a partir de análises estatísticas. A empresa tornou-se mais conhecida após trabalhar para a campanha presidencial de Donald Trump e também para o que ficou conhecido como *Brexit*, a saída do Reino Unido da União Europeia, e seu papel nestas tem sido contestado e inclusive investigado nos respectivos países.

O cerne da questão quanto à proteção da privacidade e violação dos dados pessoais, que se tornou um grande problema, foi o noticiado em março de 2018. Segundo noticiado em jornais como o The New York Times e o The Guardian, os dados de milhões de usuários do Facebook teriam sido obtidos irregularmente pela empresa a partir do aplicativo "*This is Your Digital Life",* disponibilizado na rede social. Cerca de 320 mil usuários da rede social utilizaram o aplicativo, concedendo acesso tanto às sus informações quanto às contidas nos perfis de amigos, o que fez com que mais de 80 milhões de usuários, inclusive brasileiros, fossem afetados.

Estes "*seeders",* as pessoas que fizeram o teste e concederam acesso aos seus dados pessoais, desavisadamente deram não apenas os próprios dados como

também os de pelo menos 160 amigos.[45]

Segundo Wylie, o Facebook via o que estava acontecendo, um enorme volume de dados sendo extraídos com a coleta de milhões de perfis em questão de semanas. Porém, a política da rede social permitia o uso dos dados para propósitos acadêmicos, e o responsável pelo aplicativo informou que os dados coletados teriam essa finalidade. Assim, o Facebook teria simplesmente deixado que eles continuassem com o processo.[46] No entanto, como se verificou, a finalidade pretendida com o uso destes dados foi outra completamente diferente, tendo havido inclusive a venda das informações obtidas para terceiros sem o consentimento, ou mesmo a ciência, dos titulares dos dados. Ficando caracterizada uma violação à privacidade em escala sem precedentes.

O escândalo afetou não apenas a Cambridge Analytica, como também o próprio Facebook, que teve uma perda em milhões no valor de mercado, visto o abalo na relação com os usuários, e ainda teve que adotar medidas urgentes para contornar a situação quando o caso veio a público, revisando suas políticas de privacidade e banindo a empresa de análise de dados da plataforma.

Os usuários afetados, por sua vez, foram altamente prejudicados pelo do uso de seus próprios dados. Através da "dominação informacional"[47], que inclui técnicas tais quais rumores, desinformação e o uso de *fake news,* os eleitores americanos, por exemplo, teriam sido altamente influenciados por estes recursos direcionados, o que pode ter afetado o resultado das eleições, levantando questões inclusive quanto à sua

---

[45] CADWALLADR, Carole. "'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower". The Guardian. Disponível em: < https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump>. Acesso em 2018.

[46] CADWALLADR, Carole. "'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower". The Guardian. Disponível em: < https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump>. Acesso em 2018.

[47] CADWALLADR, Carole. "'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower". The Guardian. Disponível em: < https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump>. Acesso em 2018.

legitimidade.

No caso do Brexit, o próprio Wylie disse em entrevista que isto não teria sido possível sem a atuação da Cambridge Analytica, por meio de uma publicidade minuciosamente direcionada a partir do tratamento de dados pessoais, demonstrando o impacto que pode ter o uso destes.[48]

> "... É importante porque o referendo foi ganho com menos de 2% dos votos e muito dinheiro foi gasto em publicidade na medida certa, com base em dados pessoais. Essa quantidade de dinheiro compraria milhões e milhões de impressões. Se você se dirige a um grupo pequeno, pode ser definitivo. Se você soma todos os grupos que fizeram campanha pelo Brexit, era um terço de todo o gasto. E estamos diante de algo fundamental para o modelo constitucional deste país e para o futuro da Europa. Por isso é preciso haver uma investigação sobre os indícios de que gastaram mais do que o permitido legalmente. Quem diz é alguém moderadamente eurocético. Mas as pessoas têm de poder confiar em suas instituições democráticas. Fazer trapaças é fazer trapaças. Se alguém recorre ao doping e chega em primeiro, pode ser que tivesse ganhado sem se dopar, mas a medalha é tirada dele porque enganou. A medalha é retirada porque questionou a integridade de todo o processo. Falamos da integridade de todo o processo democrático, e se trata do futuro deste país e da Europa em geral."

O CEO do Facebook, Mark Zuckerberg, reconheceu sua culpa, depois de ter testemunhado perante o congresso americano e ter sido sabatinado pelo senado, admitindo que eles não foram capazes de prever essa modalidade de ataques por meio da desinformação, com a divulgação de notícias falsas através de contas falsas, e assim ele se comprometeu publicamente a melhorar a plataforma, implantando inclusive recursos para facilitar a identificação de notícias falsas e para facilitar o entendimento das configurações de privacidade da rede social.

A Cambridge Analytica, por sua vez, não conseguiu se manter após o baque das notícias que vieram à tona, que definitivamente abalaram sua imagem

---

[48] GUIMÓN, Pablo. "O 'Brexit' não teria acontecido sem a Cambridge Analytica". El País. Disponível em: < https://brasil.elpais.com/brasil/2018/03/26/internacional/1522058765_703094.html?rel=mas >. Acesso em 2018.

globalmente, ainda que eles aleguem ter agido dentro da legalidade, a opinião pública difere diante dos fatos que foram apresentados, tendo a empresa sido alvo inclusive de ação coletiva juntamente com o Facebook, e havido sido questionada por diversos governos.

Verifica-se, portanto, necessidade crescente da regulamentação do uso de dados pessoais a fim de proteger a privacidade dos cidadãos, especialmente de empresas com plataformas que armazenam grandes quantidades de dados pessoais e *data brokers* a fim de preencher lacunas legislativas que acabam por dar espaço a verdadeiros abusos, criar sanções e ainda uma fiscalização eficiente para garantir a fiel execução da lei e os direitos da personalidade.

Assim sendo, passar-se-á a estudar o tratamento jurídico, as respostas às violações e formas de prevenção previstas legalmente, no Brasil e no direito comparado, a fim de resguardar os direitos dos usuários.

3. O tratamento jurídico da resposta às violações

Uma maior regulamentação é necessária a fim de proteger os usuários de abusos, como vistos no tópico anterior. Uma legislação protetiva e bem detalhada, especialmente se houver previsão de alguma penalidade quando não observada tende a ser um instrumento efetivo de resposta às possíveis violações.

Este tipo de legislação faz com que as empresas, obrigadas, deem maior atenção ao tema e realizem maiores investimentos no setor de segurança da informação a fim de prevenir eventuais perdas de valor de mercado com o risco de vazamentos e com o uso indevido dos dados que armazenam.

A doutrina aponta inclusive alguns princípios, importantes a serem mencionados, que vem sendo desenvolvidos e consolidados desde as primeiras gerações de leis voltadas para a proteção de dados e privacidade e que se encontram intrinsecamente ligados aos direitos fundamentais, e que se verificam presentes nas normas paradigmáticas a serem comentadas no presente capítulo. São eles:[49]

> a) Princípio da publicidade (ou da transparência), pelo qual a existência de um banco de dados com dados pessoais deve ser de conhecimento público, seja por meio da exigência de autorização prévia para funcionar, da notificação a uma autoridade sobre sua existência, ou do envio de relatórios periódicos;
> b) Princípio da exatidão: os dados armazenados devem ser fiéis à realidade, o que compreende a necessidade de que sua coleta e seu tratamento sejam feitos com cuidado e correção, e de que sejam realizadas atualizações periódicas conforme a necessidade;
> c) Princípio da finalidade, pelo qual qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de

[49] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *EJJL-Espaço Jurídico: Journal of Law, v. 12, n. 2.* p. 100-101. 2011.

seus dados. Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que se pode, a partir dele, estruturar-se um critério para valorar a razoabilidade da utilização de determinados dados para certa finalidade (fora da qual haveria abusividade);

d) Princípio do livre acesso, pelo qual o indivíduo tem acesso ao banco de dados no qual suas informações estão armazenadas, podendo obter cópias desses registros, com a consequente possibilidade de controle desses dados; após este acesso e de acordo com o princípio da exatidão, as informações incorretas poderão ser corrigidas e aquelas obsoletas ou impertinentes poderão ser suprimidas, ou mesmo pode-se proceder a eventuais acréscimos;

e) Princípio da segurança física e lógica, pelo qual os dados devem ser protegidos contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado.

Merece nota também a Carta dos Direitos Fundamentais da União Europeia, que já prevê dentro do capítulo que trata da dignidade da pessoa humana a proteção de dados como um direito fundamental. Nela se lê:

> "Artigo 8° - Proteção de dados pessoais
> 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.
> 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação.
> 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente."

Evidencia-se, portanto que a proteção aos dados é necessária para a garantia dos direitos humanos, das liberdades, e que a tendência internacional, especialmente na legislação europeia, tem sido criar mecanismos de proteção a fim de assegurar este direito conforme as novas necessidades da vida contemporânea.

Diante disto, neste tópico serão explorados alguns formatos de leis de proteção de dados em experiências internacionais e também a atual conjuntura legal brasileira neste tocante.

3.1. Diretiva Europeia 45/96/CE

Esta diretiva foi de grande importância para a proteção da privacidade nos Estado-Membros europeus. Ela confirma a proteção aos dados como uma forma de garantia dos direitos fundamentais[50] e orientava a criação de leis que abrangessem tanto o setor público quanto o setor privado, e por sua vez acabou influenciando diversos outros países, tal qual o Canadá e a Austrália na criação de suas próprias bases legais.[51]

Posteriormente foram editadas também as seguintes diretivas, de modo a expandir a regulamentação quanto aos dados para alguns setores mais específicos, são elas; a Diretiva 97/66/CE9, de 1997, cujo enfoque é o tratamento dos dados pessoais e a proteção da privacidade no setor das telecomunicações; e a Diretiva 2002/58/CE10, de 2002, que versa sobre o tratamento de dados pessoais e à proteção da privacidade nas comunicações eletrônicas.

A legislação em tela foi um dos mais significativos avanços em matéria de proteção dos dados pessoais, e consequentemente da privacidade dos cidadãos que ela contempla, conforme já mencionado anteriormente ao analisar a evolução histórica destas leis no primeiro capítulo. Esta e outras leis serviram para formar as bases do que hoje vem sido chamado pela doutrina como um verdadeiro direito fundamental à proteção de dados.[52]

---

[50] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *EJJL-Espaço Jurídico: Journal of Law, v. 12, n. 2.* p. 102. 2011.

[51] MENDES, Laura Schertel. *Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo.* p. 134. 2010.

[52] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *EJJL-Espaço Jurídico: Journal of Law, v. 12, n. 2*. p. 96. 2011.

A diretiva tratava-se de uma norma geral proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à sua livre circulação. Ela pretendia a harmonia entre seu texto e outras normas setoriais de proteção que buscassem complementar a norma mais abrangente, a fim de abarcar setores mais específicos, sendo importante em razão da construção de uma arquitetura regulatória[53], nas palavras da professora Laura Schertel, assim compelindo os demais membros a se debruçar sobre o tema e editar suas próprias normas. Nas constituições dos países europeus posteriores a ela, muitas já incluíram em seu texto a previsões quanto a esta classe de informação, como a da Grécia, Suíça, Espanha e Países Baixos. A Carta Magna de Portugal inclusive consagrou, em seu artigo 35, a proteção das informações pessoais frente às ameaças provocadas pelo uso da informática, criando assim um rol de direitos fundamentais intrinsecamente ligados à salvaguarda da dignidade da pessoa humana. [54]

Verifica-se que esta diretiva possui dois enfoques relevantes, segundo a doutrina.[55] Por um lado, ela pretende resguardar a pessoa física ao definir normas de proteção quanto ao tratamento de seus dados e, além disto, ela também pretende induzir o comércio, pois criando regras comuns, e assim harmonizando as abordagens legais, consequentemente contribui para o sistema de mercado unificado da União Europeia, eventualmente reduzindo os custos das transações.

A norma em questão aplica-se ao tratamento de dados pessoais, sendo feito de forma automatizada ou não quando contidos em um ficheiro, um conjunto estruturado de dados, ou a ele destinados tendo em vista que o risco de danos aos direitos da personalidade não está na informatização em si, mas sim na

---

[53] MENDES, Laura Schertel. *Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo*. p. 134. 2010.

[54] MENDONÇA, Fernanda Graebin. Proteção de Dados Pessoais na Internet: Análises Comparativas da Situação do Direito à Autodeterminação Informativa no Brasil e em Países Latino-Americanos. *Revista Jurídica da Faculdade de Direito de Santa Maria-FADISMA, v. 11, n. 1*. p. 298. 2016.

[55] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental *EJJL-Espaço Jurídico: Journal of Law, v. 12, n. 2.* p. 102. 2011.

potencialidade de obtenção de informações dos titulares dos dados a partir do tratamento deles. De fato, a automatização possibilita uma organização muito maior dos dados, realizando seu cruzamento a fim de obter ainda mais informações relevantes, no entanto, tal resultado pode ser obtido também sem o uso de recursos tecnológicos tão avançados. A mera organização e análise de cadastros e registros de compras de forma não automatizada pode render os mesmos resultados, porém em escala menor, mas ainda assim gerando consequências na vida dos indivíduos analisados.

Esta norma engloba os bancos de dados administrados tanto pelo poder público quanto pelo setor privado, porém, não é cabível quando o tratamento de dados tenha como objeto a segurança pública, a defesa, a segurança do Estado, suas atividades no domínio do direito penal e aquelas realizadas pela pessoa singular no âmbito de suas atividades meramente pessoais ou domésticas, como uma agenda pessoal com endereços de amigos, por exemplo, não excluído porém se o tratamento for destinado a fins comerciais.[56]

A diretiva tem como enfoque a proteção de pessoas físicas, relegando a regulamentação das pessoas jurídicas a outros instrumentos legais, seguindo, portanto, a tendência deste tipo de legislação.[57] Ela estabelece que os dados pessoais só podem ser tratados com o consentimento do titular, e este deve ser informado da operação, devendo ter direito de acesso aos dados que lhe dizem respeito que estão sendo tratados, de modo a assegurar sua correição e a licitude do mesmo, devendo lhe ser assegurado o direito a conhecer a lógica da operação realizada, desde de que isto não comprometa o segredo comercial ou a propriedade industrial, buscando assim equilibrar os direitos da personalidade com as necessidades do mercado.[58]

---

[56] Diretiva Europeia 95/46/CE, art. 3.

[57] BENNET, Colin e RAAB, Charles. The Governance of Privacy: policy instruments in global perspective. p. 11. *Cambridge: The MIT Press.* 2006.

[58] Diretiva Europeia 95/46/CE, (41)

Portanto, percebe-se que o documento foi um marco legal de grande relevância para a proteção de dados nas últimas décadas. No entanto, a sociedade evoluiu muito desde então, graças aos inúmeros avanços tecnológicos, e com isto a abordagem legal teve que ser renovada para manter-se eficiente. Assim sendo, em 2016 foi editado o Regulamento Geral Sobre a Proteção de Dados, o qual passamos a comentar.

3.2. Regulamento (UE) 2016/679 – O Regulamento Geral Sobre a Proteção de Dados (RGPD)

Esta nova regulamentação, feita para substituir a Diretiva Europeia 45/96/CE, harmonizando a legislação quanto à proteção de dados pessoais pela Europa. Trata-se de uma atualização, vez que muito mudou desde a edição daquela diretriz na década de 90, tanto a tecnologia em si quanto as formas de relacionamento entre as pessoas e ainda as táticas de mercado.

Assim sendo, vários elementos da Diretiva Europeia 45/96/CE estarão presentes no novo regulamente, repaginados e com algumas adições. Como exemplo disto, temo Grupo de Trabalho independente, previsto no artigo 29 da antiga diretiva, de caráter consultivo, voltado justamente para a proteção das garantias legalmente previstas. Ele era composto por representantes das autoridades nacionais de proteção dos Estado-Membros e tinha como atribuição emitir recomendações e pareceres, principalmente. Em maio de 2018 este grupo será substituído pelo Comitê Europeu para a Proteção de Dados, nos termos do novo Regulamento geral, que passa a ser comentado.

O objetivo principal da nova norma é dar maior controle aos cidadãos europeus sobre o tratamento de seus dados quando estiverem relacionados às ofertas de bens, serviços e ao controle de seu comportamento, nos termos do art. 3 da resolução, tanto com relação a empresas europeias quanto estrangeiras, simplificando e unificando as normas de proteção, modernizando os princípios já consagrados na Diretiva Europeia 45/96/CE.

Tendo sido promulgado em 2016, regulamento deu às empresas o prazo de dois anos para se adequar às novas exigências, passando a surtir seus efeitos plenamente em maio de 2018. O novo regulamento irá influenciar as empresas que tratam dos dados pessoais de europeus, estando elas na União Europeia ou não, e de pessoas localizadas na EU, sendo esta uma de suas maiores novidades, a extraterritorialidade.

Este regulamento inova ao incluir tanto definições quanto proteções aos dados genéticos e biométricos, além de trazer uma série de direitos, contidos no Capítulo III, para os titulares dos dados. São eles[59]:

a) Direito a transparência e informação. É garantido ao cidadão que ele possa solicitar informações quanto ao tratamento e armazenamento de seus dados. As informações fornecidas devem estar em linguagem clara e simples, podendo o responsável pelo tratamento responder perante as autoridades de controle caso não dê seguimento ao pedido. (Arts. 12, 13 e 14)
b) Direito de acesso. O titular dos dados tem o direito de obter a confirmação do responsável pelo tratamento se seus dados estão ou não sendo objeto deste processamento, e podendo então escolher quais dados pretende ceder, de que forma e para quais finalidades. (Art. 15)
c) Direito de retificação. O titular poderá solicitar a correção ou mesmo a complementação de seus dados, ajustando-os à realidade por meio de uma declaração adicional. (Art. 16)
d) Direito ao apagamento de dados (“Direito ao esquecimento”). O titular tem o direito de ter os dados que lhe dizem respeito apagados pelo responsável, sem demora injustificada, quando for alguma das hipóteses contida neste artigo. Dentre elas podemos mencionar o tratamento ilícito de dados, a retirada do consentimento, quando finda a necessidade do uso deles, quando há uma obrigação jurídica a ser cumprida. (Art. 17)

[59] *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho.* Art. 4, 1. Disponível em: http://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em 2018

e) Direito de portabilidade dos dados. Garante ao indivíduo poder receber seus dados armazenados de forma organizada, de modo que possa facilmente transmiti-los a outro responsável por tratamento de dados conforme sua vontade, que seja impedido, desde que esteja dentro das hipóteses do artigo. (Art. 20)

f) Direito de oposição. O titular dos dados tem o direito de se opor a qualquer momento negar o uso de seus dados pessoais para determinados fins, e assim o responsável pelo tratamento deve cessar o tratamento, a não ser que apresente razões imperiosas e legítimas para sua manutenção. Para efeitos de comercialização dos dados, o titular pode se manifestar quando desejar. (Art. 21)

Há ainda o direito à limitação do tratamento, segundo o qual o titular poderia limitar o uso de seus dados em algumas situações especificadas em lei (Art. 18) e a obrigação de notificação, por parte do responsável pelo tratamento, a terceiros que tenham sido destinatários dos dados caso os dados tenham sido retificados, limitados ou mesmo apagados, a fim de que estes terceiros também estejam alinhados com a política instituída e com a informação atualizada (Art. 19).

Além do mais, os dados relativos às crianças menores de 16 anos têm proteção especial, nos termos do Art. 8 da Resolução, devendo eles, a fim de resguardar sua privacidade, ter o consentimento expresso dos pais, responsáveis legais, para seu tratamento. Os Estado-Membros poderão, a seu critério, instituir uma idade inferior, desde que não seja menor que 13 anos, assemelhando-se à legislação americana neste particular.

No mais, as disposições quanto ao consentimento foram reforçadas. Agora as companhias serão obrigadas a simplificar os termos de uso e a confirmação do consentimento deverá ser feita de forma facilitada para que o usuário, de modo que ele possa visualizar também para que fins serão usados seus dados pessoais. O regulamento prevê que a retirada do consentimento deverá ser tão fácil quanto sua concessão, devendo ser apresentada uma interface amigável para que o titular dos dados possa realizar tal operação se assim desejar, vide o art. 7º.

Quanto a isto, o art. 25 do regulamento traz a ideia de “Privacy by Design”, que consiste no desenvolvimento da plataforma já estruturalmente voltada para a proteção da privacidade. Seus recursos devem ser elaborados de modo que a apresentação dos termos seja intuitiva e a interface amigável neste sentido. Ou seja, a questão da privacidade passa a ser uma parte integrante da construção da plataforma, e não um mero termo a ser adicionado posteriormente após a criação dela. O conceito já existia há anos, porém agora ele passa a ser um requerimento legal com RGPD.

O regulamento, em seu art. 5°, institui ainda alguns princípios a serem respeitados quanto ao tratamento de dados pessoais, especificando que os referidos dados devem ser objeto de um tratamento lícito, leal e transparente. Devendo ser utilizados para a finalidade especificada e também para outras se compatíveis com a finalidade original, de modo a não comprometer a segurança do titular dessas informações.

Há previsão ainda de minimização do uso dos dados, devendo seu tratamento ser limitado ao estritamente necessário para a finalidade desejada, devendo sua conservação, ainda, ser restrita ao período necessário para atingir seus fins previstos.

Assim sendo, a fim de fiscalizar se as organizações estão em *compliance* com o RGPD, o regulamento previu ainda a criação de autoridades de controle em cada país membro da União Europeia, nos termos do art. 51. Sua criação tem a finalidade de investigar denúncias e violações do RGPD. Cada Estado-Membro deverá designar seu próprio pessoal e a entidade autuará de forma independente, não estando sujeitas a influências externas e devendo seus membros ser nomeados em um procedimento transparente. O regulamento prevê ainda as competências, atribuições e poderes destas autoridades, que desempenharão papel importante na efetivação das garantias previstas no regulamento.

A experiência já acumulada quanto à proteção de dados nas últimas décadas

já comprovou ser necessária a implementação de uma autoridade administrativa a fim de exigir o cumprimento da legislação, fiscalizando àqueles que a ela se submetem e auxiliando os titulares dos direitos com vias de criar uma verdadeira cultura da privacidade.[60]

Com isto, passa-se a falar das exigências, constantes majoritariamente no Capítulo IV da resolução, mas também em outros dispositivos, às quais as empresas que tratam dados de cidadãos da União Europeia tiveram que se adequar. Dentre elas podemos mencionar a necessidade de um representante da organização para responder pela gestão de dados pessoais. Este gestor poderá ser uma pessoa física ou mesmo um departamento, que ficará encarregado de garantir que a organização que representa está alinhada com as regras do RGPD.

Além disto, passa a haver uma diretriz a ser seguida em caso de violação de dados pessoais. Caso isto ocorra, por razões internas ou por fato de terceiro, o responsável pelo tratamento deverá notificar o ocorrido à autoridade de controle competente em até 72 horas após ter tido conhecimento da violação, devendo a notificação vir acompanhada dos motivos do atraso se o prazo determinado for excedido, é a inteligência do art. 33 do regulamento. Além disto, quando tal violação representar elevado risco aos direitos e liberdade do titular dos dados, este deverá ser notificado. A instituição de tal obrigatoriedade mostra-se necessária pois, por vezes, havendo uma falha na segurança e sem a necessidade de prestação de contas, muitas empresas preferiam não divulgar informação a fim de se resguardar, tendo em vista o abalo na confiança que isto poderia gerar e com isto os eventuais efeitos no mercado, assim pondo em risco a privacidade dos titulares dos dados para manter sua imagem.

No mais, a partir do dia 25 de maio de 2018, passado o prazo de adequação ao RGPD instituído, inicia-se a fiscalização e a emissão de multas nestes novos moldes. A fim de compelir as entidades a se adequarem ao regulamento foram

---

[60] MENDES, Laura Schertel. *Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo.* p. 135. 2010.

instituídas multas que, a depender da violação, podem chegar a 20 milhões de euros ou a 4% da receita global anual da empresa infratora, o que for maior, razão pela qual muitas empresas que tem negócios com a EU, para evitar prejuízos, já se adiantaram para estar em *compliance* com o RGPD. (Arts. 83.4, 83.5 e 83.6)

A sanções poderão ser aplicadas diretamente pelo Estado-Membro europeu se a empresa infratora tiver presença física nele. Caso a empresa em questão não se encontre fisicamente no território da UE, o regulamento exige que seja designado um representante localizado dentro da União para desempenhar o papel.

Isto posto, o RGPD mostra-se uma norma extensa e que pretende uma harmonia com outras leis elaboradas pelos estados membros a fim de melhor se adequar às suas especificidades e regular setores específicos. O regulamento vem para orientar e tende a influenciar outros países, tal qual a Diretiva Europeia 45/96/CE em seu tempo, na elaboração e mesmo atualização de suas normas próprias. Além disto, dado o fator da extraterritorialidade, as empresas que pretenderem continuar negociando bens e serviços com os europeus deverão estar em *compliance* com as novas regras, e de fato, pouco antes da entrada em vigor do RGPD muitas companhias já estão notificando os usuários das alterações em suas políticas de privacidade, o que afeta usuários de fora da união europeia, mas que usufruem dos mesmos serviços, demonstrando que desde logo a norma já está tendo um impacto perceptível.

3.3. Modelo de regulação dos Estados Unidos da América

Nos EUA há diversas leis sobre privacidade e segurança da informação por todo o território nacional, e que podem ser bem diferentes entre si. As definições acerca de dados pessoais, ou mesmo as sensíveis, variam de acordo com cada regulação. À exceção dos dados pessoais de saúde, dados financeiros, estudantis, informações pessoais de crianças abaixo de 13 anos coletadas online e informações que possam ser usadas para praticar ou identificar atos criminosos ou fraudes, que por padrão são considerados dados sensíveis.

Com o grande aumento da importância da informação, e consequentemente a necessidade de se resguardar a privacidade, os Estados Unidos, através de diversas construções legislativas e jurisprudenciais deram origem a um novo conceito de *informational privacy*[61]*,* cujo foco da proteção é o direito de acesso à informação quanto aos dados armazenados em órgãos públicos e a disciplina de proteção ao crédito, conferindo maior segurança ao consumidor.

Percebe-se que modelo de proteção de dados norte-americano é, portanto, estruturalmente diferente do europeu, já comentado. No modelo americano o processamento de dados é permitido, favorecendo o livre mercado, a não ser que isto cause algum dano ou que seja expressamente limitado pela lei americana. Na UE o que ocorre é o contrário, a regulação do tratamento de dados é detalhada, prevendo as hipóteses em que ele é permitido e ainda como deve ser feito.

Diferentemente do panorama europeu, não há uma lei maior que sirva como diretriz para as normas setoriais. Há, porém, duas leis básicas quanto à política interna, o *Fair Credit Reporting Act*, de 1970, e o *Privacy Act*, de 1974. A primeira aplica-se à emissão de relatórios sobre os consumidores, para fins de análise de perfis quanto ao risco de crédito, seguros e contratação de empregados. Já a segunda trata das empresas ou agências governamentais que administram um sistema de registro para o governo. [62]

Quanto à política externa, diante das diferenças entre os Estados Unidos e a União Europeia, porém, e tendo em vista que o fluxo internacional de dados entre os dois era de suma importância para as relações comerciais[63], eles negociaram o *Safe Harbor Agreement of 2000* que, em poucas palavras, deveria proteger os

---

[61] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. p. 94. *EJJL-Espaço Jurídico: Journal of Law, v. 12, n. 2.* 2011.

[62] MENDES, Laura Schertel. *Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo.* p. 142. 2010.

[63] MELTZER, Joshua Paul. The Internet, Cross-Border Data Flows and International Trade. *Asia & the Pacific Policy Studies, v. 2, n. 1.* p. 90-102. 2015.

dados de cidadãos europeus se estes fossem guardados por companhias americanas para serem tratados nos EUA. No entanto, o acordo foi invalidado pela EU, em 2015 o Tribunal de Justiça da União Europeia reconheceu que o referido acordo não alcançava os padrões de proteção de dados da EU. Como isto, muitas empresas que estavam sob a égide daquele acordo tiveram que implementar medidas alternativas. Esta invalidação criou certa insegurança jurídica e muitos temiam que isto pudesse afetar os negócios já estabelecidos.[64]

Em resposta à situação, em 2016 o acordo foi revisado, dando origem ao *Privacy Shield,* que já foi elaborado com certa influência do RGPD e é consideravelmente mais longo e detalhado que seu antecessor. Esta legislação contém uma série de princípios, principalmente com relação às transações comerciais, mas também quanto aos dados sensíveis e inclusive quanto ao papel das autoridades responsáveis pela proteção dos dados. Assim, as empresas americanas que pretendam trabalhar com os dados de cidadãos europeus têm que se comprometer a estar em *compliance* com este padrão estabelecido.

Os EUA têm uma forte regulamentação quanto à privacidade dos dados para o setor público. O Privacy Act de 1974, seria um exemplo de legislação aplicável somente à esfera federal, e ainda sim tendo sua abrangência limitada, conforme leciona Colin Bennett.[65] O setor privado, por outro lado, apenas agora tem sido alvo de maior atenção, especialmente após o escândalo do tratamento desvirtuado dos dados do Facebook pela empresa Cambridge Analytica. Dada a forte base liberal norte-americana, no entanto, a intervenção do estado tende a ser mínima, mesmo com o icônico caso, já abordado no capítulo 3, as previsões são de que as providências tomadas pelo governo americano não sejam extensivas como na União Europeia.

---

[64] WEISS, Martin A.; ARCHICK, Kristin. *US-EU data privacy: from safe harbor to privacy shield*. 2016. Disponível em: < https://epic.org/crs/R44257.pdf >. Acesso em 2018.

[65] MENDES, Laura Schertel. *Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo.* p. 134. 2010.

Quanto aos menores de 13 anos de idade, conforme já mencionado, há uma lei específica, o *Children's Online Privacy Protection Act.* Esta lei pretendeu regular a coleta de informações dos menores sites comerciais na Internet, criando uma série de deveres para os operadores destas plataformas. Por exemplo, há a necessidade de que seja obtido o consentimento dos responsáveis pela criança para que seus dados sejam coletados, em caso de solicitação dos responsáveis os operadores deverão responder que tipo de tratamento foi feito com os dados de seus filhos e ainda mediante solicitação, a fim de proteger a integridade e a privacidade dos menores, os responsáveis podem pedir para seja impedida a coleta e a divulgação dos dados de seus filhos.

Isto posto, em razão dos avanços tecnológicos ocorridos desde a edição da lei em 1998 entendeu que o regulamento precisava ser atualizado. Foram feitas emendas, tendo ela sido reformulada em 2013, considerando a nova realidade das redes sociais, dos dispositivos móveis com geolocalização e outros novos recursos utilizados que poderiam ser potencialmente invasivos. No entanto, está em discussão um projeto para renovar completamente o referido ato, dado que alguns já consideram a legislação atual insuficiente, apesar das mudanças, e sugerem a introdução de uma nova norma.[66]

Assim sendo, percebe-se que os Estados Unidos, com seu sistema fortemente federalista e com um alinhamento marcadamente liberal, preferiram regulamentar alguns setores e ditar regras poucas regras padrão para toda a nação em vez de criar um regulamento único e muito detalhado, como no modelo europeu. Ainda assim, porém, o país optou por fazer concessões, vide o *Privacy Shield*, de modo a se alinhar com a política internacional a fim de manter boas relações com o mercado europeu.

Percebe-se, portanto, uma tendência geral de harmonização entre as normas

[66] MATECKI, Lauren A. COPPA is Ineffective Legislation! Next Steps for Protecting Youth Privacy Rights in the Social Networking Era. *Northwestern Journal of Law & Social Policy, Volume 5, Issue 2.* 2010. Disponível em: http://scholarlycommons.law.northwestern.edu/njlsp/vol5/iss2/7. Acesso em 2018

internacionais no tocante à proteção dos dados pessoais, especialmente em razão do fluxo de dados facilitado pela internet, o que permite uma troca de grande monta entre países. Assim, se inclusive os Estados Unidos investiram em políticas de compliance para continuar mantendo relações, principalmente de mercado, a tendência é que a legislação brasileira também seja influenciada pela legislação internacional.

3.4. Regulação em países da América Latina

Diferentemente do Brasil, vários países da América Latina já possuem um arcabouço jurídico mais avançado no tocante à proteção de dados pessoais, mostrando-se especialmente inspirados pelo modelo europeu. Diante disto, alguns exemplos merecem ser mencionados, mostrando a experiência dos países mais próximos.

O Uruguai possui a Lei 18.331/2008, que trata tanto da proteção de dados quanto do *habeas data* no país. Nesta, a garantia da proteção de dados é tida como um direito fundamental, remetendo à sua própria Constituição, razão pela qual o país foi inclusive reconhecido pela União Europeia como um país juridicamente avançado no tema, tendo inclusive sido convidado pela UE a aderir à Convenção 108 da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), que traz em seu texto os princípios essenciais da proteção de dados, e assim sendo considerado apto a receber os dados dos cidadãos europeus.[67] Quanto à Lei 18.331/2008, assim se lê no art. 1º:

> *"Artigo 1º - O direito à proteção dos dados pessoais é inerente à pessoa humana, motivo pelo qual está compreendido no artigo 72 da Constituição da República"*

O Chile, por sua vez, publicou a Lei 19.628 em 1999, sendo o primeiro país

[67] MENDONÇA, Fernanda Graebin. Proteção de Dados Pessoais na Internet: Análises Comparativas da Situação do Direito à Autodeterminação Informativa no Brasil e em Países Latino-Americanos. *Revista Jurídica da Faculdade de Direito de Santa Maria-FADISMA,* v. 11, n. 1. p. 298. 2016.

da América Latina a regular esta matéria, abrangendo assim tanto normas procedimentais quanto substantivas, conforme leciona Fernanda Graebin Mendonça, prevendo desde a necessidade de autorização do uso dos dados por seus titulares à adstrição de seu uso para a finalidade informada e pactuada, dentre outros. A referida lei foi atualizada em 2012 para se adequar aos novos desafios que a internet apresentou ao potencializar a transferência de dados.[68]

Outro exemplo latino é a Argentina, cuja Lei 25.326/2000 foi editada a fim de tutelar o uso das informações pessoais no ambiente virtual.[69] Eles exploraram os temas basilares, desde os conceitos, às garantias conferidas e eventuais sanções em caso de descumprimento da lei. Eles buscaram inspiração também no modelo europeu, tendo a sua legislação sido considerada adequada quanto ao tema e, portanto, assim como o Uruguai os dados de europeus podem ser transferidos para o país sem maiores empecilhos.

E por fim, a título de comparação, há o caso do México, que por sua vez, mostra-se consideravelmente avançado com relação aos demais países já enunciados. Ele tem a Lei Federal de Proteção de Dados Pessoais em Posse de Particulares, de 2010, sendo ela bem mais recente que as outras mencionadas e, portanto, mais completa, trazendo os conceitos de dados, consentimento e outras com a finalidade de regular seu tratamento legítimo. Além de possuir alguns estados que já criaram sua própria legislação local quanto ao tema, como é o caso do Distrito Federal e do estado de Coahuila. Mas antes mesmo destas leis, a Constituição mexicana já havia sido editada a fim de criar medidas de proteção aos dados pessoais de seus cidadãos, incluindo o direito à autodeterminação informativa no seu rol de garantias, juntamente com direitos humanos, em 2007, tendo havido ainda outras reformas posteriormente que aumentaram ainda mais as previsões,

---

[68] CHILE. SOBRE PROTECCION DE LA VIDA PRIVADA Disponível em: < https://www.leychile.cl/Navegar?idNorma=141599>

[69] MENDONÇA, Fernanda Graebin. Proteção de Dados Pessoais na Internet: Análises Comparativas da Situação do Direito à Autodeterminação Informativa no Brasil e em Países Latino-Americanos. *Revista Jurídica da Faculdade de Direito de Santa Maria-FADISMA,* v. 11, n. 1. p. 305. 2016.

especialmente garantias, concedidas aos titulares de dados pessoais. A Carta Magna do México é considerada pela doutrina um documento bem trabalhado neste quesito.[70]

Diante das experiências brevemente comentadas nos países latinos, e tendo em vista a crescente necessidade de se debruçar sobre o tema, dado o novo contexto tecnológico regido pelo *Big Data,* verifica-se que vários países, inclusive os de histórico semelhante ao Brasil, já tratam ou estão em discussão para regulamentar o assunto. Segundo um levantamento feito por Graham Greenleaf, professor da Law & Information Systems, UNSW Australia, em janeiro de 2015 já eram 109 países com leis voltadas para a proteção da privacidade dos dados.[71] O cenário no Brasil, ainda não avançou muito no tema, sendo que o Marco Civil alcança apenas os requisitos mínimos de uma lei com este enfoque, e tem seu escopo mais voltado para os dados no meio virtual. Ainda assim, há outros recursos no ordenamento jurídico brasileiro que já proporcionam uma base para uma maior regulamentação, como será explorado no capítulo a seguir.

3.5. Regulação do uso de dados pessoais no Brasil

Ainda não há uma regulamentação específica no Brasil no tocante à proteção do uso de dados pessoais, porém, o país tem previsões esparsas na legislação que buscam proteger a privacidade e os dados pessoais. É possível identificar princípios correlatos na Constituição, velando pela vida privada, intimidade e o direito à informação, bem como no Código Civil, ao abordar os direitos da personalidade, no Código de Defesa do Consumidor, quanto aos cadastros de crédito e, recentemente, de forma mais específica, mas ainda pendente de lei mais detalhada, no Marco Civil da Internet.

---

[70] MENDONÇA, Fernanda Graebin. Proteção de Dados Pessoais na Internet: Análises Comparativas da Situação do Direito à Autodeterminação Informativa no Brasil e em Países Latino-Americanos. *Revista Jurídica da Faculdade de Direito de Santa Maria-FADISMA*, v. 11, n. 1. p. 305. 2016.

[71] GREENLEAF, Graham. *Global data privacy laws 2015: 109 countries, with european laws now a minority.* 2015. Disponível em: < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2603529>

Na Constituição da República, em seu art. 5°, X considera invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas. No inciso XI ela põe a salvo especificamente os dados, afirmando que são invioláveis o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo por ordem judicial, na forma que a lei estabelecer. E também, no inciso LXXII a Carta Magna prevê a possibilidade do *habeas data* para possibilitar o conhecimento de informações pessoais, e mesmo a retificação delas. Doneda ensina ainda que o habeas data foi introduzido pela Constituição de 1988 com um propósito de cunho fortemente humanitário e com inspiração na experiência estrangeira.

> "Cabe ressaltar que o habeas data brasileiro surgiu basicamente como um instrumento para a requisição das informações pessoais em posse do poder público, em particular dos órgãos responsáveis pela repressão durante o regime militar e sem maiores vínculos, portanto, com uma eventual influência da experiência europeia ou norte--americana relativa à proteção de dados pessoais, já em pleno desenvolvimento à época" [72]

Verifica-se, portanto, que há uma preocupação com a privacidade e com a segurança das informações dos cidadãos a ponto de incluí-los entre os direitos e garantias fundamentais, servindo como base para a legislação infraconstitucional.

Quanto à legislação infraconstitucional, o Código de Defesa do Consumidor traz algumas previsões quanto a bancos de dados e cadastros, vide seu art. 43, onde dispõe sobre a obrigatoriedade de acesso do consumidor às aos seus próprios dados armazenados, a necessidade dos cadastros serem de fácil compreensão e transparentes, a possibilidade de retificação dos dados neles contidos e inclusive as obrigações dos responsáveis de não fornecer informações que possam impedir ou dificultar o acesso ao crédito destes consumidores quando findo o prazo prescricional para a cobrança de eventuais débitos. Ainda que de forma mais rudimentar, e assim complementada pela doutrina e jurisprudência, o Brasil já

[72] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *EJJL-Espaço Jurídico: Journal of Law*, v. 12, n. 2. p. 103-104. 2011.

apresenta alguns recursos para resguardar a privacidade e a dignidade da pessoa humana na seara consumerista.

Mais recentemente, foi introduzido o Marco Civil da Internet, Lei 12.695, que foi um grande avanço no campo da normatização do meio virtual, trazendo em seu texto tanto princípios quanto garantias e direitos para este campo, que merecem menção posto que norteiam a forma como deverá ser feito o tratamento de dados.

> "Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
> a) justifiquem sua coleta;
> b) não sejam vedadas pela legislação; e
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
> IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
> X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;"

Pelas previsões contidas no rol dos direitos, a regulamentação a ser elaborada, conforme previsão do art. 3º, III, do Marco Civil, devem se aproximar do modelo adotado pelos europeus, dando maior controle aos usuários sobre o uso de seus próprios dados, restringindo o acesso de terceiros e demandando um consentimento livre e informado do titular quando este for autorizar seu uso. Porém, o país ainda carece de uma regulamentação mais densa.

> "Isto posto, o Brasil encontra-se em situação delicada, principalmente após os escândalos de espionagem norte-americana – caso Snowden – quando foi possível constatar que o país

> está despreparado para lidar com possíveis violações de dados pessoais, mesmo que a jurisprudência já tenha se posicionado acerca de casos sobre dados pessoais e algumas leis já tenham articulado sobre o assunto, as decisões ainda são contraditórias e as leis abordam o tema de forma superficial ou específica para apenas um setor, deixando todos os outros casos desprotegidos.” [73]

Pela experiência estrangeira, constata-se que a forma mais eficaz de proteger a privacidade é justamente através de leis gerais direcionadas especificamente para isto.[74] Diante disto, já há no Brasil algumas iniciativas legislativas voltadas para realizar esta regulamentação.

O mais antigo deles, e também o menos protetivo até então, era o PL 4060/2012. Ele permitiria o tratamento dos dados pessoais, mas sem as necessárias autorizações dos titulares e ainda sem maiores garantias quanto à segurança e mesmo a transferência destes dados. Um ponto positivo do projeto é que a proposta excluiria a atividade jornalística de seu âmbito de aplicação, visando garantir a liberdade de expressão, mas sem discorrer muito sobre o tema.

Por outro lado, o projeto não mencionava a Lei de Acesso à Informação, podendo criar uma brecha legislativa para que o poder público possa prejudicar sua necessária transparência. Não previa a criação de um órgão regulatório independente a fim de fiscalizar e implementar as proteções aos dados nele previstas, tampouco estabelecia quais órgãos públicos ficariam responsáveis por estes encargos, implicando basicamente em uma auto-regulamentação. Não havia previsão de mecanismos de controle por parte da sociedade ou mesmo e tratava vagamente do tema dos dados sensíveis, limitando-se a dar definições vagas de sua natureza e características além de permitir uma autorização genérica para a utilização de tais dados, o que poderia ser incluído em contratos longos e de

---

[73] SOUZA, LUÍZA RIBEIRO DE MENEZES. Proteção de Dados Pessoais: Estudo Comparado do Regulamento 2016/679 do Parlamento Europeu e Conselho e o Projeto de Lei Brasileiro N. 5.276/2016. *Caderno Virtual*, v. 1, n. 41, 2018.

[74] MENDES, Laura Schertel. *Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo.* p. 133. 2010.

linguagem inacessível, sem qualquer destaque, dificultando a identificação das permissões de utilização de dados altamente relevantes por parte de seus titulares.

Como se vê, o projeto ia na contramão do progresso até então alcançado com as atuais leis, especialmente se comparada com o panorama europeu já abordado, assim focando no tratamento dos dados, porém pecando nas proteções necessárias para que o processamento se dê de forma justa a fim de evitar violações aos direitos da personalidade.[75] Assim, outro projeto, mais abrangente, foi apresentado.

O PLS 330/2013 já contava com mais garantias. Ele proibia o tratamento de dados pessoais sensíveis, ressalvando algumas exceções. Quanto ao consentimento do titular, este projeto previa que este deveria ser livre, específico, inequívoco e informado, e especialmente destacado quando relativo ao tratamento dos dados sensíveis, devendo ser explicitada a finalidade do seu tratamento e inclusive se seus dados seriam repassados a terceiros.

Este projeto demonstrava maior preocupação com a segurança, demandando que os responsáveis pelo tratamento se atualizassem com recursos técnicos condizentes com os padrões internacionais e que em caso de falha na segurança, havendo um vazamento destes dados, por exemplo, o incidente deveria ser comunicado detalhadamente ao órgão competente para a adoção de providências.

Houve, no entanto, algumas críticas ao projeto. Por exemplo, ele não faz o contrabalanço entre a privacidade dos titulares dos dados e o direito à liberdade de expressão, consideração necessária posto que os dois direitos invariavelmente aparecem em conflito e que a lei desde já poderia criar algumas previsões. Além do mais, este projeto não faz menção à Lei de Acesso à Informação, tornando o projeto de certa forma perigoso, tendo em vista que a lacuna legislativa deixada pode dar

[75] BANISAR, Dave. GUILLEMIN, Gabrielle. BLACO, Marcelo. *Proteção de dados pessoais no Brasil: Análise dos projetos de lei em tramitação no Congresso Nacional.* p. 39-43. 2016.

espaço para interpretações que favorecem o sigilo em órgãos públicos quanto ao uso de dados pessoais. No mais, o projeto também não avalia a criação de um órgão independente que pudesse fiscalizar o tratamento de dados, deixando isto a cargo do poder público.[76]

Por estes e outros fatores, o PLS 330/2013 se mostrou insuficiente, sendo praticamente superado por outro projeto. Foi então apresentado o PL 5276/2016, inspirado no modelo europeu, sendo ele o mais recente e abrangente destes três.

O PL 5276/2016 prevê maiores garantias quanto ao tratamento de dados realizado com os cidadãos brasileiros, tanto quando feito por empresas públicas quanto por empresas privadas. Seu maior diferencial com relação aos outros, ao menos em sua elaboração, foi a ampla consulta pública realizada, inclusive realizada em plataforma online do governo, a fim de angariar e incluir em seu texto sugestões de toda a sociedade.

Este projeto, diferentemente dos anteriores, pretende a atribuição de um órgão responsável por fiscalizar a fiel aplicação e observância de seu texto, tendo sido considerado satisfatório em alguns pontos, como por exemplo; a menção à liberdade de expressão, já equilibrando-a com o direito à privacidade e excetuando a atividade jornalística de seu âmbito de aplicação, reduzindo a possibilidade de utilização da lei para fins de censura; a expressa previsão de proteção aos dados sensíveis, limitando seu tratamento a algumas situações e requerendo uma autorização específica para o uso destes, que são mais delicados no tocante à privacidade de seu titular; o projeto faz as necessárias menções à Lei de Acesso à Informação, informando como deve ser feito o tratamento por pessoas jurídicas de direito público e ainda como deve ser o compartilhamento destes dados com as entidades de direito privado; o projeto ainda aborda os graus de consentimento que o titular pode dar para o uso de seus dados e suas repercussões, o quão transparente o responsável pelo tratamento deve ser, e como deve ser

[76] BANISAR, Dave. GUILLEMIN, Gabrielle. BLACO, Marcelo. *Proteção de dados pessoais no Brasil: Análise dos projetos de lei em tramitação no Congresso Nacional.* p. 32-38. 2016.

supervisionado pelo órgão competente e pelo titular dos dados, podendo este requisitar a retificação deles, denunciar eventuais violações perpetradas ou mesmo revogar o seu consentimento para o uso.

Outro fator que merece menção foram as previsões quanto à transferência internacional de dados. O projeto de lei prevê que tal transferência e o uso destes dados em países estrangeiros, que é normal dado o uso da internet, só poderá ser realizada naqueles onde houver um nível de proteção ao menos semelhante, considerados alguns requisitos previstos em lei.

O projeto também não cria um órgão de controle e fiscalização das medidas propostas pela lei, mas já indica a criação de um conselho de proteção dos dados pessoais, semelhante ao modelo europeu contido no RGPD.

Porém, o projeto ainda precisa de melhorias. Foram feitas algumas críticas a seu respeito pois apesar de ele representar um significativo avanço quanto a proteção à privacidade no âmbito nacional, ele não abarca algumas hipóteses relevantes que já foram tratadas no âmbito internacional.

Em avaliação feita por especialistas, algumas deficiências foram detectadas. A Artigo 19, organização não governamental que atua na defesa e promoção da liberdade de expressão e do acesso à informação, em um estudo comparativo feito quanto aos projetos de lei em análise, apresentou algumas recomendações para o PL 5276/2016, tendo em vista alguns dos aspectos identificados como insatisfatórios.

Primeiramente, o PL 5276/2016 poderia vir a ser mal interpretado no que toca o direito ao esquecimento, que se encontra entre suas previsões. Sem maiores especificações, ou delimitações, esta garantia poderia ser utilizada para excluir informações que são de interesse público, pessoas conhecidas poderiam ocultar dados relevantes sob o argumento da proteção da sua privacidade utilizando-se dos novos recursos da lei quanto aos dados pessoais. Assim, a ONG sugere que o PL faça uma ressalva explícita quanto à defesa do interesse público nos dispositivos

tratarem da exclusão ou cancelamento do uso de dados.[77]

No mais, são feitas algumas outras recomendações, como a necessidade de aprofundamento das leis quanto ao órgão regulatório que ficará responsável pela sua supervisão e consequentemente sua efetivação. Além disso, é sugerido que haja uma delimitação do uso de dados para realização de pesquisa estatística, pois da forma como fora proposto é possível que tal recurso legal seja usado para justificar um tratamento dos dados de forma desvirtuada

No final de maio de 2018, porém, influenciados pela entrada em vigor do RGDP, o PL 4060/2012 veio a ser profundamente alterado, tendo o PL 5276/2016 sido a ele apensado juntamente com o PL 6.291/16, que propõe uma alteração do Marco Civil. O projeto de lei de 2012 foi sancionado na Câmara dos Deputados, tendo sido aprovado por meio de um substitutivo mais robusto que incorporou diversas alterações, sendo algumas delas comentadas em seguida.

O projeto passou a prever a necessidade de um consentimento específico e em destaque para finalidades específicas quanto ao uso dos dados sensíveis, e sendo eles apenas os relativos a pessoas naturais, não se subsumindo a esta exigência, portanto, os dados anonimizados. Todavia, a lei passa a prever um rol restrito de hipóteses onde não será necessário o consentimento, vide o art. 11 do projeto. Além disso, criou previsões específicas para o uso dos dados de saúde no art. 13, permitindo seu uso para estudos quanto à saúde pública, limitando-os à finalidade específica da pesquisa e obrigando sua manutenção em ambiente seguro.

Abordou o chamado legítimo interesse, vide o art. 10, que consiste em uma das hipóteses do tratamento de dados sem a necessidade do consentimento prévio, tanto para não onerar demais o titular com a reiterada necessidade de manifestação do consentimento quanto para atender a alguma finalidade pública ou privada

[77] BANISAR, Dave. GUILLEMIN, Gabrielle. BLACO, Marcelo. *Proteção de dados pessoais no Brasil: Análise dos projetos de lei em tramitação no Congresso Nacional.* p. 25-31. 2016.

legítima, como para prevenir fraudes bancárias e garantir maior segurança.

O substitutivo ampliou a seção acerca do tratamento de dados relativo a crianças e adolescentes, exigindo o consentimento específico e em destaque por pelo menos um dos pais para que os dados sejam utilizados, prevendo a possibilidade de uso não consentido a fim de contatar os pais da criança em questão, por exemplo.

Já nos artigos 23 a 30 do projeto foi feita uma compatibilização deste com a Lei de Acesso à Informação, abordando o tratamento de dados pessoais pelo poder público, buscando proteger e preservar os dados pessoais de requerentes de acesso a informações públicas (Art. 23, II) e conferir maior transparência do serviço público (Art. 25), determinando sua estruturação de modo que o acesso aos dados públicos seja facilitado.

No mais, o projeto passa a tratar da criação de um órgão competente independente, em seu artigo 54, a Autoridade Nacional de Proteção de Dados. Este funcionará como uma espécie de agência reguladora com a finalidade de fiscalizar a fiel execução da lei, nos termos dos arts. 52 e 53, criando a possibilidade de aplicação de advertências, multas e inclusive suspensão ou mesmo proibição do banco de dados.

Estas são apenas algumas das mudanças contidas no projeto, que em razão disto agora tramita na forma de um substitutivo. Segundo o autor, a lei pretende um equilíbrio, evitando a exposição das pessoas e protegendo seus dados, ao mesmo tempo que não barra os avanços tecnológicos, sendo ela necessária para atender às atuais necessidades do país, tanto internamente quanto com relação à política externa. A Europa, por exemplo, exige um nível de proteção mínimo aos dados pessoais de seus cidadãos para que estes possam ser tratados por outros países, o que demonstra a importância de uma regulamentação a fim de atender demandas que extrapolam as fronteiras.

Vale lembrar que o Brasil acaba se submetendo também a algumas normas

internacionais nesta seara. O RGPD europeu, por exemplo, se aplica às empresas brasileiras que atendem àqueles da União Europeia, e em razão disto elas devem se adequar às suas exigências a fim de manter boas relações negociais e evitar eventuais sanções, como as próprias multas previstas no regulamento. Tendo isto em vista, mesmo os cidadãos que não pertencem à EU devem se beneficiar dos novos termos de uso e políticas de privacidade oferecidas pelas empresas, especialmente as do ramo de tecnologia que oferecem seus serviços na internet, tendo em vista que são feitos obedecendo a um padrão aplicável a todo os usuários.

Diante do exposto, feitas as devidas considerações acerca do panorama nacional da legislação quanto à proteção de dados, verifica-se que o país ainda precisa se aprofundar nesta questão. A internet facilita um fluxo de dados transnacional de grandes proporções, e por esta razão, mesmo no tocante à regulação feita internamente, não se pode deixar de haver um diálogo internacional a fim de alinhar a legislação neste tocante, aprendendo com a experiência externa e oferecendo maior proteção a todos os titulares de dados pessoais da melhor forma possível, equilibradamente, sem que lhes seja negada a participação na sociedade lhes faltando serviços essenciais e ao mesmo tempo sem permitir que sua intimidade seja violada.

Conclusão

Ao longo deste estudo foram analisados tópicos importantes quanto à proteção dos dados pessoais. Para tanto, inicialmente foi feito um histórico da legislação relativa à proteção da privacidade quanto aos dados pessoais e a influência da evolução da tecnologia, bem como a conceituação de relevantes termos para a correta compreensão do tema abordado no presente trabalho.

Em seguida, foram feitas considerações acerca das violações que podem ser perpetradas, de que forma elas podem ocorrer atualmente e ainda seus potencias efeitos lesivos ao titular dos dados ou mesmo à coletividade como um todo, ao ser possível influenciar as massas com base nos perfis construídos, sendo possível até mesmo ter um papel decisivo em eleições, como no caso da Cambridge Analytica comentado neste tópico.

Por fim, foram analisadas algumas das normas existentes mais relevantes nesta seara, comentando-se o cenário europeu, o dos Estados Unidos e o de alguns países latino-americanos, e como estas normas internacionais poderiam vir a influenciar inclusive a legislação brasileira, tanto como fonte de inspiração para a criação de uma lei de proteção de dados quanto nas próprias relações internacionais, tendo em vista a crescente necessidade de harmonização entre elas, dado o crescente compartilhamento de dados entre países, especialmente por meio da internet. Realizou-se, portanto, que uma lei de proteção de dados no Brasil é uma necessidade crescente, especialmente diante das exigências internacionais, como novos padrões de proteção, e em razão de casos como o da Cambridge Analytica, conforme estudado.

Considerando as violações que podem ocorrer, ameaçando direitos fundamentais da personalidade, e necessário que se dê a atenção jurídica necessária ao tratamento e a consequente necessidade de proteção dos dados pessoais.

No Brasil, em especial, onde a proteção à intimidade e à vida privada são

direitos constitucionalmente protegidos, deve ser elaborada uma regulamentação adequada que seja eficiente para a proteção dos cidadãos e que ao mesmo tempo não engesse o mercado. Deve-se buscar, portanto um equilíbrio entre ambos, e para tanto não só é possível como necessário buscar inspiração na legislação internacional atual bem como em suas experiências pretéritas.

Constata-se que atualmente o direito, em muitos casos, precisa estar alinhado com as políticas internacionais, e isto é essencial quanto à matéria da proteção de dados tendo em vista que a internet possibilita um fluxo de dados transnacional de grande monta. Ou seja, os dados de um usuário argentino, localizado no Brasil podem estar sendo tratados nos Estados Unidos, por exemplo, o que demanda uma regulamentação quanto aos dados deste titular e inclusive um diálogo entre as leis de diversos países a fim de prever respostas jurídicas eficientes, e de modo coordenado, que preservem os direitos fundamentais do titular quanto ao uso de seus dados.

Quanto a isto, verificou-se no estudo que o RGPD criou um novo padrão e demanda um nível de proteção de dados mínimo para que empresas e afins possam tratar os dados dos europeus. Diante disto, as empresas, e mesmo países, que pretendem continuar negociando com o mercado europeu terão que se adequar a estas exigências. Fazer concessões se torna uma realidade necessária, por exemplo, mesmo os Estados Unidos criaram previsões como o *Privacy Shield* a fim de responder adequadamente às demandas do mercado europeu.

Assim, conclui-se que o Brasil deve seguir a tendência internacional preponderante, alinhando-se com as normas europeias, tal qual os outros países da América Latina, tendo em vista a análise feita dos projetos de lei que tramitam atualmente, que buscam conferir maior controle do cidadão sobre o uso de seus próprios dados, e que há uma necessidade imediata de regulamentação deste tema no país, sendo que isto deve ganhar maior visibilidade em razão de casos como o da Cambridge Analytica e das mudanças ocorridas em outros ordenamentos jurídicos, como é o caso do RGPD.

REFERÊNCIA BIBLIOGRÁFICAS

BANISAR, Dave. GUILLEMIN, Gabrielle. BLACO, Marcelo. *Proteção de dados pessoais no Brasil: Análise dos projetos de lei em tramitação no Congresso Nacional.* 2016. Disponível em: < http://artigo19.org/wpcontent/blogs.dir/24/files/2017/01/Prote%C3%A7%C3%A3o-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf >. Acesso em 2018.

BENNET, Colin e RAAB, Charles. The Governance of Privacy: policy instruments in global perspective. Cambridge: *The MIT Press*, 2006.

CASTELLS, Manuel; MAJER, Roneide Venâncio; GERHARDT, Klauss Brandini. *A sociedade em rede.* Fundação Calouste Gulbenkian, 2002.

COELHO, Luiz Fernando. *Teoria Critica do Direito.*3ª Edição. Belo Horizonte. Del Rey, 2003. p. 277

DA ROSA, Tais Hemann; FERRARI, Graziela Maria Rigo. Privacidade, intimidade e proteção de dados pessoais (aspectos brasileiros). *Argumenta Journal Law*, n. 21, p. 137-166, 2015.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *EJJL-Espaço Jurídico: Journal of Law*, v. 12, n. 2, p. 91-108, 2011.

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

GARFINKEL, Simson. *Database nation: the death of privacy in the 21st century.* O'Reilly Media, Inc., 2000.

GERMAN, Christiano. *O caminho do Brasil rumo à era da informação.* Konrad-Adenauer-Stiftung. 2000.

KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. Private traits and attributes are predictable from digital records of human behavior*. Proceedings of the National Academy of Sciences*, v. 110, n. 15, p. 5802-5805, 2013. Disponível em: < http://www.pnas.org/content/110/15/5802.short > Acesso em 2018.

LINS, Bernardo F. E. Privacidade e internet*. Estudo técnico da Consultoria Legislativa. Brasília: Câmara dos Deputados/Consultoria Legislativa.* 2000.

MATECKI, Lauren A. COPPA is Ineffective Legislation! Next Steps for Protecting Youth Privacy Rights in the Social Networking Era. *Northwestern Journal of Law & Social Policy,* Volume 5, Issue 2. 2010. Disponível em:

http://scholarlycommons.law.northwestern.edu/njlsp/vol5/iss2/7

MELTZER, Joshua Paul. The Internet, Cross-Border Data Flows and International Trade. *Asia & the Pacific Policy Studies*, v. 2, n. 1, p. 90-102, 2015.

MENDES, Laura Schertel. *Privacidade, Proteção de Dados e Defesa do Consumidor.* Saraiva. 2014.

MENDES, Laura Schertel. *Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo*. 2010. Disponível em: < http://www.repositorio.unb.br/bitstream/10482/4782/1/DISSERTACAO%20LAURA.pdf > Acesso em 2017

MENDONÇA, Fernanda Graebin. Proteção de Dados Pessoais na Internet: Análises Comparativas da Situação do Direito à Autodeterminação Informativa no Brasil e Em Países Latino-Americanos. *Revista Jurídica da Faculdade de Direito de Santa Maria-FADISMA*, v. 11, n. 1, p. 283-311, 2016.

PASSOS, Bruno Ricardo dos Santos. *O direito à privacidade e a proteção aos dados pessoais na sociedade da informação: uma abordagem acerca de um novo direito fundamental.* 2017.

PINHEIRO, Patrícia Peck. Direito digital. Saraiva. 2016.

PEISSL, Walter; KRIEGER-LAMINA, Jaro. The scored consumer: privacy and big data. In: *International Conference on Consumer Research (ICCR)*. DEU, 2017. p. 101-112.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. O direito à proteção de dados pessoais na sociedade da informação. *Revista Direito, Estado e Sociedade*, n. 36, 2010.

SOUZA, LUÍZA RIBEIRO DE MENEZES. Proteção de Dados Pessoais: Estudo Comparado do Regulamento 2016/679 do Parlamento Europeu e Conselho e o Projeto de Lei Brasileiro N. 5.276/2016. *Caderno Virtual, v. 1, n. 41*, 2018. Disponível em: < https://portal.idp.emnuvens.com.br/cadernovirtual/article/view/3153 >. Acesso em 2018.

VIEIRA, Tatiana Malta. *O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação.* 2007.

WARREN, Samuel; BRANDEIS, Louis. The right to privacy. *Harvard Law Review*, v. 4, n. 5, p. 193-220, 1890. Disponível em: <

http://www.jstor.org/stable/pdf/1321160.pdf?refreqid=excelsior%3A8c00c00b2e2c0c87e1676989f6c46858 > Acesso em 2018

WEISS, Martin A.; ARCHICK, Kristin. *US-EU data privacy: from safe harbor to privacy shield.* 2016. Disponível em: < https://epic.org/crs/R44257.pdf >. Acesso em 2018.

WENDT, Emerson; FREITAS, Lidiane Marques; CALHEIROS, Tânia da Costa. *Dados Sensíveis: uma análise do Art. 5º, Inciso III, do PL nº 5276/2016 para a proteção de dados pessoais.* 2017. Disponível em: < http://direitoeti.com.br/site/wp-content/uploads/2017/10/WENDT-FREITAS-CALHEIROS_Dados-Sens%C3%ADveis.pdf> Acesso em 2018.

WERTHEIN, Jorge. A sociedade da informação e seus desafios. *Ciência da informação, Brasília*, v. 29, n. 2, p. 71-77, 2000.