UNIVERSIDADE CATÓLICA DE SANTOS
MESTRADO EM DIREITO INTERNACIONAL

SILAS ANTUNES DE CARVALHO GAVETTI

A ORGANIZAÇÃO INTERNACIONAL PARA A PROTEÇÃO DE DADOS PESSOAIS COLETADOS NA INTERNET EM ESCALA GLOBAL

SANTOS
2021

UNIVERSIDADE CATÓLICA DE SANTOS
MESTRADO EM DIREITO INTERNACIONAL

SILAS ANTUNES DE CARVALHO GAVETTI

A ORGANIZAÇÃO INTERNACIONAL PARA A PROTEÇÃO DE DADOS PESSOAIS COLETADOS NA INTERNET EM ESCALA GLOBAL

Dissertação apresentada à banca de defesa da Universidade Católica de Santos, como requisito para conclusão do curso de mestrado em Direito Internacional.

Área de concentração: Direito Internacional.
Orientador: Prof. Dr. Daniel Freire e Almeida

SANTOS
2021

[Dados Internacionais de Catalogação]
Departamento de Bibliotecas da Universidade Católica de Santos

---

G282o Gavetti, Silas Antunes de Carvalho
A Organização Internacional para a Proteção de Dados Pessoais Coletados na Internet em Escala Global / Silas Antunes de Carvalho Gavetti ; orientador Daniel Freire e Almeida. -- 2021.
83 f.; 30 cm

Dissertação (mestrado) - Universidade Católica de Santos, Programa de Pós-Graduação stricto sensu em Direito Internacional, 2021
Inclui bibliografia

1. Direito internacional. 2. Proteção de dados. 3. Internet. 4. Organização internacional I.Almeida, Daniel Freire e. II. Título.

CDU: Ed. 1997 -- 34(043.3)

Viviane Santos da Silva - CRB 8/6746

SILAS ANTUNES DE CARVALHO GAVETTI

A ORGANIZAÇÃO INTERNACIONAL PARA A PROTEÇÃO DE DADOS PESSOAIS COLETADOS NA INTERNET EM ESCALA GLOBAL

Dissertação apresentada à Faculdade de Direito da Universidade Católica de Santos para obtenção do título de Mestre em Direito.

Santos, 18 de fevereiro de 2021.

BANCA EXAMINADORA

_____

Prof. Dr. Daniel Freire e Almeida
Universidade Católica de Santos

_____

Prof. Dr. Rodrigo Luiz Zanethi
Universidade Católica de Santos

_____

Prof. Dr. Rodrigo Luiz Zanethi
Universidade Católica de Santos

À memória de meu avô
Sylvio Antunes de Carvalho.

RESUMO

A presente dissertação tem como objetivo apresentar uma organização internacional que tenha como premissa a expansão da proteção de dados pessoais mundialmente de maneira uniforme. A internet é global por natureza e se utiliza primordialmente da coleta e processamento de dados dos usuários para operar um modelo econômico com base na exploração desses dados para direcionar publicidade aos usuários. Diante de questões sobre como os Estados nacionais desenvolvem legislações eficazes neste ínterim, sobre como a proteção dos usuários de internet ocorre quando não há legislação específica e como é possível imaginar uma proteção uniforme mundialmente, é apresentada a hipótese da organização internacional para a proteção de dados pessoais. Este estudo faz uso do método hipotético dedutivo e a pesquisa referencial bibliográfica para justificar esta hipótese, visando demonstrar os alguns pontos. Primeiramente, as características da internet que criam o problema narrado, sua extraterritorialidade, a presença de empresas gigantes que definem o setor e a economia com base na vigilância. O segundo ponto abarca os conflitos entre jurisdição que a internet já produziu e que dificultam a eficácia de uma solução por meio de jurisdições nacionais. O terceiro é a proteção de dados pessoais como um direito fundamental e um direito humano, que deve ser protegido em todo mundo. O projeto também aborda exemplos de como as jurisdições nacionais estão lidando com o problema, seja mantendo a internet livre e global, ou uma internet repleta de fronteiras digitais. Apresenta também a organização hipotética em suas características, o papel dos Estados dentro da organização e a obrigação de internalizar sua legislação, bem como um mecanismo de cooperação interestatal, o papel das empresas, com direito à voz dentro da organização, um selo para demonstrar cumprimento das normas acordadas e as penalidades em caso de descumprimento. Por fim, aborda a participação dos usuários, seja a partir de organizações não governamentais dentro da entidade, seja por um sistema de peticionamento para pareceres.

Palavras-chave: Proteção de dados pessoais. Internet. Organização internacional.

ABSTRACT

This aim of this paper is to present an international organization that has as a premise the expansion of the worldwide and uniform personal data protection. The internet is naturally global and is primarily used to collect and process user data to operate an economic model based on the exploitation of that data to target advertising to users. Faced with questions about how national states develop effective legislation in the meantime, about how the protection of internet users occurs when there is no specific legislation and how it is possible to imagine uniform protection worldwide, the hypothesis of the international organization for personal data protection is presented. This study is based on the hypothetical deductive method and bibliographic referential research to justify this hypothesis, aiming to demonstrate some points. First, the characteristics of the internet that create the narrated problem, its extraterritoriality, the presence of huge companies that define the sector and the economy based on surveillance. The second point covers conflicts between jurisdictions that the internet has already produced and that hinder the effectiveness of a solution through national jurisdictions. The third is the protection of personal data as a fundamental human right, which must be protected worldwide. The project also addresses examples of how national jurisdictions are dealing with the issue, whether it is keeping the internet free and global, or an internet full of digital boundaries. It also presents the hypothetical organization in its characteristics, the role of States within the organization and the obligation to internalize its legislation, as well as an interstate cooperation mechanism, the role of companies, with the right to a voice within the organization, a seal to demonstrate compliance agreed rules and penalties for non-compliance. Finally, it addresses the participation of users, whether from non-governmental organizations within the entity, or through a system of petitioning for opinions.

Keywords: Protection of personal data. Internet. International organization.

SUMÁRIO

1 INTRODUÇÃO

A presente dissertação de tem como objetivo demonstrar uma hipótese para três questões: Como as novas leis de proteção de dados pessoais, criadas por legislações nacionais ou com jurisdição territorialmente limitada, podem dar conta de solucionar com eficácia o processamento de dados na internet, que é global por natureza? Como fica a proteção de usuários de localidades que nas quais não existem tais legislações, uma vez que se trata de um direito de todos? Por fim, como garantir que essa proteção seja uniforme em todos os lugares, para todos os usuários, sem criação de fronteiras digitais ou paraísos para o processamento dos dados?

Recentemente, foram criadas leis para a proteção de dados pessoais de grande relevância, sendo elas, primordialmente, a *General Data Protection Regulation*, a lei 2016/679 da União Europeia, a Lei Geral de Proteção de Dados brasileira, a lei número 13.709/2018, além da *California Consumer Privacy Act* (CCPA), desenvolvida na Califórnia, e outras legislações relevantes em países como Índia, China, Chile, Argentina e Uruguai. Com isso, despertou-se o interesse sobre o direito de proteção de dados pessoais, em especial diante da massiva utilização desses dados no ambiente digital, reforçado por casos recentes de grandes questões envolvendo a coleta massiva de dados pessoais e casos de grande relevância que fazem questionar a privacidade na rede.

Ao estudar o *digital* em ambiente digital, toma-se conhecimento de dinâmicas próprias do ciberespaço. Como a internet, global por natureza, é capaz de criar situações não pensadas pelas jurisdições nacionais? Essas novas leis detém os mecanismos necessários para possuir eficácia nesse ambiente? Como o direito de proteção de dados é um direito da personalidade, ele é tratado como direito fundamental pela União Europeia, como um direito próprio, e está relacionado com direito à privacidade, segurança, dignidade e outros direitos humanos.

Ao refletir sobre esses pontos, cria-se a hipótese de uma organização internacional que irá levar em conta as características próprias da internet. Tal organização internacional teria como objetivo promover uma unificação em como as legislações nacionais tratam o direito de proteção de dados pessoais. Ela também buscaria uma resolução mais adequada à velocidade da internet para os problemas que envolvem os dados pessoais. Para demonstrar tal hipótese, foram usados o

método hipotético dedutivo e a pesquisa referencial bibliográfica para a elaboração do presente trabalho.

O primeiro capítulo tem o objetivo de demonstrar quais são as características que são únicas da internet e criam as dificuldades apresentadas no problema. A primeira característica apontada é a extraterritorialidade, que demonstra a arquitetura global da internet, pois ela permite trocas, comunicação, comércio, relacionamentos e conflitos simultâneos em todo o planeta. A segunda característica é a massiva presença de entes privados no controle dos ambientes da internet, falando de gigantes que dominam a internet, com usuários de seus sistemas em todo o mundo, coletando, processando e armazenando dados desses usuários, sem necessariamente estar territorialmente presente na mesma localização do usuário. Essas empresas são riquíssimas e têm alcances gigantescos de usuários, com grande poder dentro e fora da internet. Por fim, é apontado o novo modelo econômico baseado na exploração de dados criado na internet, com atores privados que se valem deste formato para gerar sua riqueza. Neste molde, os serviços são prestados gratuitamente, em troca dos dados pessoais para a promoção de publicidade direcionada ao usuário com base em sua própria experiência. Os dados pessoais são a nova moeda dessa economia.

O segundo capítulo tem como foco os problemas que os sistemas jurídicos nacionais têm enfrentado ao longo da história para lidar com a internet. Nem sempre as decisões jurídicas sobre fatos *on-line* atingiram uma prestação jurisdicional adequada ou eficaz. Elencam-se, então, casos que provam a necessidade da solução global para problemas na internet. Faz-se isso para questionar se as legislações nacionais sobre dados pessoais processados no ambiente digital não enfrentaram os mesmos obstáculos.

Já o terceiro capítulo aborda a questão dos dados pessoais como um novo direito fundamental, independente, e não apenas uma divisão do direito à privacidade. Reforça tal posicionamento com a demonstração e o reconhecimento da proteção de dados como um direito fundamental na União Europeia, bem como momentos em que a proteção de dados pode ser acionada mesmo sem ser uma questão que envolva dados privados. É importante entender a proteção de dados dessa forma para ter a perspective sobre por que o problema da dissertação entende como necessária uma abrangência global das regulações de dados pessoais.

Assim, apresentamos os sistemas atuais de proteção de dados e como eles tentam contornar as dificuldades promovidas pelas características da internet apontadas no primeiro capítulo. Como a lei europeia, a brasileira e a indiana se preocupam em cuidar da proteção de dados, levando-se em consideração a internet global. É necessário também abordar a solução encontrada pela China para o controle da internet e como pode estar sendo criadas fronteiras para a internet.

Apresentamos a hipótese desse trabalho desejando a manutenção de uma internet global. Tal hipótese é apresentada levando em consideração todos esses fatores, defendendo a criação de uma organização internacional com a ambição de uniformizar a proteção de dados pessoais no mundo. Para os Estados, ela pretende criar a obrigação de internalizar uma legislação de proteção de dados que se adeque aos princípios adotados pela instituição. Esses princípios devem ser voltados à proteção do usuário em seu direito da personalidade, mas não deve restringir a atuação global das empresas. O foco da proteção deve ser no usuário, sem impedir os avanços que a ciência de dados foi capaz de proporcionar ao consumidor. É uma solução que visa entender o problema por um viés que se sustente nos mecanismos de governança global, com participação ampliada e descentralizada. Ela também deverá ter um papel de autoridade supervisora da atuação das empresas na coleta e manipulação dos dados. Não será, entretanto, um órgão judicial global para a internet. Apenas uma espécie de agência reguladora da atuação dessas empresas e dos Estados. Para tanto, a própria presença das empresas nas decisões da organização é de vital importância. Deverá ser criado um mecanismo de bonificação pela participação da empresa na organização, ao mesmo tempo em que irá criar instrumentos de punição pelo uso inadequado dos dados pela empresa.

Por fim, a organização deverá criar uma forma de peticionamento direto dos usuários para reclamar o bom uso dos seus dados. Também, faz-se necessário uma forma de cooperação global das empresas detentoras dos dados com as jurisdições estatais, sem a necessidade de uma carta rogatória. E, por fim, um sistema de transparência quanto aos dados detidos pelas empresas ou Estados para com seus usuários.

2 A INTERNET E SUAS CARACTERÍSTICAS QUE DESAFIAM LEGISLAÇÕES

O peso da internet é inegável no cotidiano de todo o mundo. A vida social, profissional, os hábitos de consumo, o controle financeiro, entretenimento, busca por conhecimento ou informação atualizada, relações de amizade e, algumas vezes, amorosos: todos têm ramificações ou estão inteiramente inseridos na internet.

Neste trabalho, serão discutidas algumas características importantíssimas da internet, que compõem o que é atualmente chamado de *ambiente digital*. Também é abordada a possibilidade de uma solução global que entenda a internet além das jurisdições nacionais, a fim de promover a proteção de dados pessoais, que são a base do negócio de instituições, afetando um grande número de pessoas ao mesmo tempo em todo mundo. Neste ínterim, também será debatida a forma de promover a proteção de dados globalmente em qualquer jurisdição, mantendo a internet livre e global.

Chega-se a essa abordagem em razão de algumas características próprias da internet: sua extraterritorialidade, a presença de organizações transnacionais que dominam o setor de forma quase oligárquica e o entendimento próprio do direito dentro da internet. Fala-se de segurança, privacidade, liberdade, transparência, expressão e muitos outros direitos humanos afetados pela forma que os dados são manipulados na internet. Além disso, será discutido como promover a proteção de dados pessoais como um direito humano a ser tratado uniformemente em todos os lugares.

Tendo estabelecidos o tamanho e a importância da presença da internet no mundo, é necessário pontuar que ela não está livre de riscos. Desde os pioneiros do estudo do direito na internet, como, por exemplo, Lawrence Lessig (2006, p. 20), já se percebeu que ela traria desafios novos a serem enfrentados pelos legisladores.

O ambiente digital permite uma dualidade, que duas vidas ocorram: uma virtual, uma real. Parte desta dualidade sempre é virtual, porém, é a parte correspondente a vidas que antes era impossíveis, inconvenientes ou incomuns. O problema é que algumas dessas vidas provocam repercussões fora do ambiente da internet, tanto para outras pessoas conectadas como para pessoas à sua volta. O que irá obrigar uma resposta dos legisladores fora do ambiente virtual.

Neste cenário, surgem leis que visam regular o ambiente virtual. Um exemplo no direito brasileiro do marco civil da internet é a Lei 12.965/2014 e, mais recentemente, a Lei Geral de Proteção de Dados Pessoais (LGPD), número 13.709/2018. São leis criadas para tentar levar o direito à internet, e a eficácia dessas

legislações e seus desafios serão debatidos no decorrer do trabalho. Porém, é inegável a importância legislativa do Marco Civil, bem como seu caráter inovador, pois trouxe uma maior afirmação de direitos e políticas públicas, garantindo princípios básicos ao bom uso da internet. (PECK, 2018, p. 35)

A priori, será abordada a importância da internet para o mundo do direito, em especial dos direitos humanos. A Organização das Nações Unidas (ONU) reconheceu o poder que a internet tem em acelerar o progresso pelo desenvolvimento como uma ferramenta inigualável à disseminação de informação e conhecimento, estabelecendo a educação como a peça-chave para isso. É o que consta no comunicado da 32ª sessão do *Human Rights Council* (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 2016).

Por meio do referido documento, a ONU convoca seus Estados membros para promover a alfabetização digital, com o intuito de promover acesso à informação, riquíssima na internet, além de promover a cooperação internacional para o desenvolvimento em todos os países da instalação de mídia de informação e comunicação.

A organização faz a ressalva da importância de se assegurar os direitos humanos também dentro do ambiente da internet, protegendo a liberdade de expressão, de associação, privacidade, entre outros pontos, fazendo isso por meio de instituições nacionais democráticas, transparentes, com o intuito de garantir liberdade e segurança aos indivíduos na internet. Nessa via de mão dupla entre a internet como ferramenta de promoção de direitos humanos e ainda sim tentando proteger os indivíduos de dentro do ambiente digital, a ONU condenou quem impede ou obstaculiza a disseminação de informação via internet, por ser uma violação à legislação internacional de direitos humanos (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 2016).

2.1 A EXTRATERRITORIALIDADE

O alcance da internet no mundo é impressionante, principalmente nos países considerados mais desenvolvidos. Quase toda a população está conectada dentro do ambiente digital. Essa afirmação está apoiada nos números publicados pela *Internet World Stats*. No ano de 2019, mais da metade da população mundial encontra-se

conectada. Estamos falando de 57,3% das pessoas na Terra, 4.536.248.808 de cidadãos, em 30 de junho de 2019 (INTERNET WORLD STATS, 2019).

Como foi dito, nos países mais desenvolvidos, a internet encontra-se mais difundida, enquanto nas regiões mais pobres o acesso ainda é mais restrito. Na Europa, 86,8% da população tem acesso à internet, assim como a América do Norte há 89,4% da população conectada, com um crescimento no número de usuários entre os anos 2000 e 2019 de impressionantes 592% para Europa e de 203% para América do Norte (INTERNET WORLD STATS, 2019).

Em outras regiões, percebemos um crescimento muito elevado do número de usuários. Na Ásia, por exemplo, há 54,2% de sua população conectada, o que representa um número impressionante de 2.300.469.859 usuários. América Latina e Caribe têm 68,9% de sua população conectada, e o Oriente Médio tem 67,9%. Por fim, a Oceania tem 68,4% de sua população conectada ao ambiente digital (INTERNET WORLD STATS, 2019).

Com tantas pessoas conectadas ao mesmo tempo, trocando informações e se relacionando com qualquer um que esteja em qualquer lugar do mundo, a internet cria um ambiente interligado a nível global. Para ela, tirando exceções, as fronteiras não têm qualquer significância. É um ambiente global por natureza, capaz de gerar conflitos de lei e jurisdição. Este é o efeito da internet como uma aldeia global (PECK, 2018, p. 32).

A Internet surge como um fórum para a coesão social, discussões democráticas e como uma plataforma de informação, entretenimento, comunicação, comércio e governança (FREIRE E ALMEIDA, 2015, p. 373), considerando uma escala mundial e simultânea. Assim, como explica Castells (2011, p. 431), a internet é a espinha dorsal da comunicação global. É a rede que liga a maior parte das redes. Em suas diversas formas e evoluções, a internet já é o meio de comunicação interativo universal via computador da Era da Informação (CASTELLS, 2011, p. 433).

Ao se referir ao período em que a televisão era o principal instrumento de comunicação em massa, Castells (2011, p.426) ensina que não se vivia em uma aldeia global, mas em domicílios sob medida, globalmente produzidos e localmente distribuídos. Já para a internet, os consumidores são também produtores de conteúdo e dão forma à teia.

Hoje, existem milhões de usuários da rede no mundo inteiro, cobrindo todo o espectro da comunicação humana. Uma fatia cada vez maior da internet vai se tornando uma grande feira. Uma parte considerável das comunicações da internet acontece de forma espontânea não organizada e diversificada em finalidade e adesão. A coexistência pacífica de diversos interesses e culturas tornou a *World Wide Web*, ou *www*, uma rede flexível formada por outras redes dentro da internet, na qual instituições, empresas, associações e pessoas físicas criam os próprios sítios, que servem para que cada usuário possa criar sua página própria. A criação do *www* tornou, literalmente, uma teia de alcance global para comunicação individualizada e interativa (CASTELLS, 2011, p. 439-440).

São criadas, assim, comunidades não físicas e que não seguem o mesmo de comunicação e interação de comunidades físicas, porém, que existem em outro plano da realidade. São comunidades criadas por laços fracos, diversificados e especializados, capazes de gerar reciprocidade e apoio por intermédio de dinâmica de interação sustentada. São capazes de transcender distâncias a baixo custo, de natureza assincrônica, combinam comunicação em massa com a penetração da comunidade individual e permitem diversas afiliações em comunidades parciais. Os vínculos cibernéticos oferecem a oportunidade de vínculos sociais para pessoas que, de outra forma, viveriam isoladas, já que seus vínculos são cada vez mais especialmente dispersos (CASTELL, 2011, p. 445-446).

A internet e seu novo sistema de comunicação transformam radicalmente o espaço e tempo, bem como as dimensões fundamentais da vida humana. Com a proximidade que ela proporciona, as localidades perdem suas características culturais, históricas e geográficas, e reintegram-se em redes funcionais ou em colagem de imagens. Assim, o espaço virtual de troca de informações substitui o espaço de físico (CASTELLS, 2011, p. 462).

Portanto, pela primeira vez na história das civilizações, um indivíduo ou uma empresa pequena tem alcance fácil e, mesmo dispondo de poucos recursos, não só tem acesso a informações localizadas nos mais distantes pontos do globo, como também pode criar, conectar, contratar, gerenciar, comparar, disponibilizar e distribuir produtos em larga escala. Antes, isso só era atingível por grandes empresas de porte multinacional (FREIRE E ALMEIDA, 2015. p. 373). Esse é o poder da internet de

reduzir fronteiras: transformar em global algo que antes só era possível em âmbito local. Esse é o sentido da extraterritorialidade da internet.

No século XXI, a internet se torna cada vez mais a principal ferramenta de comunicação intensamente usada no mundo inteiro. Surgem, então, diversas redes sociais - como *Google*, *Youtube*, *Facebook*, *Orkut*, *Twitter* e *Linkedin* – nas quais qualquer um pode tomar conhecimento de publicações sobre a vida dos usuários, seus preconceitos, gostos, ideias, políticas, além da possibilidade de adicionar pessoas em seu círculo, postar fotos, *links* e jogos. As possibilidades são infinitas nas *benditas* ou *malditas* redes sociais. *Bendita* por ser uma forma rápida e prática de contatar o mundo, seja qual for o motivo; *maldita* porque muitos se utilizam dessa rede para denegrir a imagem humana, disseminando imagens íntimas ou ofensas morais (TRENTIN; TRENTIN, 2012, p. 82).

O Brasil não se encontra distante desta aldeia. Em dados disponibilizados pelo Instituto Brasileiro de Geografia e Estatística (IBGE), o país já tem acesso à internet em 74,9% dos lares em 2017, sendo que, em 2016, este número era apenas de 69,3%. Mais relevante ainda é o número de pessoas com à internet por meio do aparelho celular. São 93,2% dos lares brasileiros com acesso a celulares, dos quais 97% são utilizados para conectar a internet.

O IBGE ainda dá destaque a como a internet está presente na vida da população mais jovem, mais vulnerável aos riscos da tecnologia. Para pessoas acima de 10 anos de idade, temos 69,8% de pessoas que já acessaram, ao menos uma vez na vida, a internet. Para pessoas entre 20 e 24 anos, ela está presente em 88,4% da população (INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA, 2018).

Vimos que, tradicionalmente, o território sempre foi definido por dois aspectos que são quebrados no ambiente digital: os recursos físicos que o compõem ou, então, a abrangência que determinada cultura está disseminada em um espaço. O território no ambiente digital é dificilmente demarcável. A riqueza está baseada na informação, que é inesgotável e pode ser infinitamente duplicada. Ao mesmo tempo, a internet permite que diferentes culturas se comuniquem o tempo todo. Um exemplo é que não o fato de não ser necessário deslocar-se para a Turquia para pessoas de qualquer outro local se relacionar com alguém daquele país. Assim como pode se entender a cultura no sentido mais amplo, como, por exemplo, a maneira que indivíduos realizam acordos comerciais ou questão jurídicas. Pode ser importante entender a cultura local

de forma mais profunda do que se um indivíduo estivesse fisicamente localizado em território turco. Fica clara, então, a possibilidade de conflitos e choques culturais causados pelas relações globais que a internet proporciona. Assim, o Direito Digital requer uma existência e um entendimento global (PINHEIRO, 2013, p. 49).

O exemplo supracitado demonstra a característica da extraterritorialidade na internet. Ela espalha globalmente a informação, sua maior riqueza, e permite a comunicação direta de culturas completamente diferente, para o que, antes, seria necessária uma viagem longa para poder ter contato. Tudo está simplificado de dentro de casa, ou a todo momento no bolso, em um celular. Isso cria a primeira dificuldade para atuação do direito na internet, a aplicação de jurisdição adequada e eficaz.

Pensando nisso, o Direito Internacional já apresentou algumas medidas para que se entenda sua aplicabilidade. A Organização do Tratado do Atlântico Norte criou o *Tallin Manual.* Trata-se de uma coleção de regras vistas como costumeiras e aplicáveis ao ciberespaço. O documento dispõe que nenhum Estado pode arrogar soberania total sobre o ciberespaço, apenas sobre as ciberinfraestruturas e as atividades relacionadas a elas, desde que localizadas em seu território. É uma aplicação da soberania territorial ao ciberespaço.

Assim, conclui-se que a ciberinfraestrutura (por exemplo, servidores ou banco de dados) localizada em um território está submetida a esta jurisdição, protegida contra a interferência dos demais (ARGA E LIMA; CARVALHO, 2019, p. 64-65). Conclui-se também que o Estado pode exercer sua jurisdição de três formas: sob agentes que fazem parte de operações do ciberespaço em seu território, sob as infraestruturas baseadas em seu território e extraterritorialmente, e de acordo com o direito internacional. Aqui, razões de aplicação podem ser a nacionalidade do agente, nacionalidade da vítima, violações de normas de direito internacional ou motivos de segurança nacional. Por fim, é possível a aplicação da doutrina dos efeitos, em que se permite a aplicação de jurisdição de fato ocorrida no estrangeiro, mas com efeitos no território soberano (ARGA E LIMA e CARVALHO, 2019, p. 64-65). Como a premissa do presente trabalho dita, a internet gera conflitos que testam esses princípios, em especial, quando ele provoca o choque entre duas jurisdições distintas.

2.2 A IMPORTÂNCIA DE ATORES PRIVADOS

A segunda característica da internet que agrava a dificuldade que o direito encontra na internet é o protagonismo de empresas privadas. As organizações que atuam no ambiente digital têm um alcance global, incorporando uma quantidade enorme de usuários dos seus serviços ao mesmo tempo em todo mundo. Grande parte delas está situada no Vale do Silício, porém, existem outras localizadas na China, por exemplo, onde a cultura e as políticas são completamente diferentes.

Demonstra-se o poder desses gigantes quando falamos sobre o *Google*, que opera nove em cada dez pesquisas online na internet em todo o mundo. Também cé válido citar o *Facebook*, a rede social de maior difusão no mundo com mais de dois bilhões de usuários espalhados em todos os cantos. Essas duas organizações detêm mais da metade do mercado publicitário online. Temos também a *Apple*, que iniciou como uma indústria de computadores, e evoluiu para operar a mais lucrativa loja de aplicativos móveis, dominando 80% deste mercado, além de deter o segundo maior negócio para o *streaming* de música, com um terço também deste mercado. A *Amazon* é responsável por quase toda venda de mercadorias online nos Estados Unidos. Estas empresas são chamadas, por seu tamanho gigantesco, de “superfirmas”, e por serem capazes de assegurar grandes parcelas do mercado, traduzindo seu poder em lucros enormes (MAYER-SCHONBERG; RAMGE, 2018, p. 48).

Neste ambiente no qual a riqueza é medida pela informação, surgem alguns nomes da lista da Forbes dos dez mais ricos do mundo. A começar por Jeff Bezos, CEO da *Amazon*. Sua fortuna está estimada em 131 bilhões de dólares, que superou Bill Gates da *Microsoft*, o segundo colocado, com 96,5 bilhões. Há também, em oitavo na lista, Mark Zuckerberg, famoso idealizador do *Facebook*, detentor de uma fortuna de 62,3 bilhões de dólares. Assim como o décimo lugar da lista, Larry Page, CEO do *Google*, com 50,8 bilhões. Esses citados superam diversos mercados tradicionais, gerando sua riqueza dentro do ambiente da internet (ALMEIDA, 2019).

Porém, a maior característica do sucesso dessas empresas é a detenção de um mercado dentro de si mesmo, e não meras lojas. Repetindo alguns dos exemplos de cima, a plataforma da *Amazon* negocia mais de US$ 200 bilhões em mercadorias, compradas e vendidas, a cada ano. A *Apple* controla um mercado gigantesco para música, vídeo e *software*. O *Spotify*, maior serviço de *streaming* de música do mundo, oferece o maior mercado deste setor. Já a superfirma de *e-commerce chinesa Alibaba* gerencia o maior mercado de negócios, entre outros negócios *business-to-business*

do planeta. Enquanto isso, o *Google* e o *Facebook* são o maior espaço publicitário do mundo, além de ser a maior ferramenta de busca e, respectivamente, a maior plataforma de mídia social do planeta (MAYER-SCHONBERG; RAMGE, 2018, p. 49).

São essas superfirmas que atuam na internet e se beneficiam do alcance global que ela lhe proporciona. São elas que disseminam informação e recolhem informação do mundo inteiro, transformando-as em imensas quantidades de riqueza.

Assim, ao se observar esses dois aspectos já citados, começou a se pensar como o direito iria encarar a internet para além dela propriamente dita, como também os espaços virtuais que existem dentro dela, o ciberespaço. No mundo desconectado, o direito está estruturado de forma já conhecida, por constituições, estatutos e outros códigos legais. A lei em sentido amplo. Porém, dentro do ciberespaço, a regulação está em primeiro lugar no *software* e no *hardware* que criam este ambiente. Estamos falando do código-base deste ciberespaço. Por essa razão, o pioneiro dos estudos do direito na internet Lawrence Lessig cunhou a afirmação “código é lei” (LESSIG, 2006, p. 5).

Há no ciberespaço alguns ambientes que permitem maior regulação do que outros. Algumas arquiteturas mais reguláveis e outras menos, permitindo maior ou menor controle. Assim, se uma parte da internet, ou toda ela, pode ser regulada, a regulação gira em torno da natureza da arquitetura do código base em que foi escrito. De tal modo, a arquitetura do código base afeta a qual comportamento pode ser controlado (LESSIG, 2006, Pag. 24).

Quem detém o controle sobre a arquitetura do código do seu ambiente dentro da internet é aquele que o escreve. Sendo assim, dentro do *Facebook*, ele mesmo é capaz de criar o código que permite ou não determinado comportamento em seu ciberespaço. O desafio do legislador do mundo real é criar leis que consigam, de forma eficaz, influenciar a organização a construir um código que respeite essa legislação. Ao mesmo tempo, a legislação pode ser escrita pelo país de um indivíduo, porém, o código foi pensado para uma legislação diversa, já que a organização está localizada em país diverso. Cria-se um choque de jurisdição.

Levando em conta a proteção de dados pessoais, sabendo que a riqueza deste mundo é a informação, há a possibilidade do conflito entre a jurisdição do Estado que reside o indivíduo com a organização que recolhe e processa esses dados, que pode operar simultaneamente uma infinidade de informações sobre pessoas de todo o

mundo ao mesmo tempo. Esses aspectos serão debatidos com mais profundidade no decorrer do presente trabalho.

2.3 A NOVA ECONOMIA BASEADA EM DADOS CRIADA PELA INTERNET

Após tecer esse comentário sobre a internet em si, é preciso abordar as questões que envolvem diretamente os dados pessoais e como ele é utilizado na internet pelas organizações. Aqui, se aborda a relevância que a informação tem para ser considerada a riqueza do mundo digital.

Primeiro, é necessário diferenciar dados de informação. Estes não são equivalentes, apesar de, em diversas vezes, serem tratados quase como sinônimos. O dado não agrega conhecimento por si. São apenas fatos brutos que precisam passar por um processamento e serem organizados, de forma inteligível, para ser possível extrair determinada informação. Para isso que servem os bancos de dados. Sua dinâmica, seja um automatizado por meio de um *software* ou não, requer a entrada do fato bruto no sistema, o processamento do dado e, a partir daí, a extração da informação que se deseja (BIONI, 2019, p. 37).

Ademais, abordam-se quais são esses dados coletados. Quando um cadastro é feito em algum serviço, são gerados dois tipos de informação. A primeira é os dados cadastrais, inseridos diretamente ao preencher o formulário de inscrição. Em segundo e mais importante, são os dados comportamentais, obtidos a partir do uso do serviço. Tudo é registrado. Seja a escolha de alimentos em um supermercado atrelado ao uso de um plano de fidelidade e descontos com identificação a partir do CPF, sejam opiniões expressadas em redes sociais ou que são buscadas e lidas pelo indivíduo, seja via *Facebook*, *Twitter*, um portal de notícias ou canais do *Youtube* (PINHEIRO, 2013, p. 52).

É desta forma que os dados repercutem nas características debatidas no item anterior deste trabalho. Os mercados existem há milênios, não sendo novidade criada na era dos dados, mas os mercados criados dentro do ambiente digital pelas gigantes digitais da atualidade não operam de forma tradicional. Eles são riquíssimos em dados de todos seus usuários espalhados por todo o mundo. Esses dados são utilizados para melhorar as transações realizadas nesse ambiente, gerando benefícios e melhorias à vida dos consumidores. Quanto mais dados existem sobre os produtos

em ofertas e sobre as preferências dos consumidores que utilizam determinada plataforma, além dos vendedores que estão se utilizando deste mercado para chegar até o consumidor, mais o consumidor encontrará aquilo que está procurando. Isso também permite que as empresas descubram cada vez mais novas formas de aperfeiçoar o atendimento aos seus clientes, com promoções e oportunidades baseadas no comportamento dos indivíduos (MAYER-SCHONBERG; RAMGE, 2018, p. 49).

Essa é a maior evolução para o mercado de consumo trazido pelo amplo processamento de dados que existem hoje em dia. Lawrence Lessing (2006, p. 287) explica que sua relação com um centro comercial é diferente dos mercados no ciberespaço. Se não o cliente não gosta de um supermercado, irá em outro. O poder é a capacidade de deixar o local. Se o serviço não lhe agrada, busca-se outro e o que os faz trabalhar bem é a competição entre eles. No ambiente da internet, essa relação está conturbada, já que essas superfirmas detêm seus mercados dentro de si e o caráter social destes só faz sentido quando abrangem o maior número de pessoas possível.

Aliás, esta evolução representa outra ferramenta importante que esses mercados possuem. É oferecido aos usuários um assistente de decisão digital. Esta ferramenta é capaz de peneirar enormes quantidades de informação com o intuito de fornecer ao consumidor recomendações, com a ressalva de serem muitas vezes supérfluas, para as escolhas que os clientes fazem. São esses assistentes automatizados que compilam dados de comportamento de clientes e comparam com o comportamento de outros clientes e permite que, por exemplo, o *Spotify* recomende músicas, que o *Netflix* faça sugestões de filmes, ou a *App Store* da *Apple* sugira aplicações. Essa ferramenta se prova de extrema importância para essas organizações quando um terço das vendas de varejo da *Amazon* é resultante dos consumidores seguirem o conselho da ferramenta de assistente de decisão automatizada criada pela empresa (MAYER-SCHONBERG; RAMGE, 2018, p. 49).

Isso só se torna possível graças ao advento do que é chamado de *Big Data*, o êxtase da mineração de dados. É um progresso quantitativo e qualitativo de gestão de informação a partir da mineração de dados. O *Big Data* é uma metodologia de processamento de dados em que se processam informações antes inimagináveis e

em diversos formatos, seja texto, imagem, áudio e outros, com o diferencial de uma altíssima velocidade.

Ele não analisa os dados em pequenas amostragens, mas sim percorre uma análise de toda a extensão dos dados disponíveis. A partir deles, são desvendados padrões de comportamento e consegue auferir a probabilidade de acontecimentos futuros. Assim, o *Big Data* não está preocupado com a causa de determinado evento. Não é um estudo de causalidade. Ele busca desvendar a probabilidade da ocorrência de eventos, não a causa dos mesmos (BIONI, 2019, p. 42).

A eficácia desses sistemas de predição com base na mineração de dados se prova de altíssima eficácia quando se verifica a comprovação da possibilidade de medir a opinião pública por meio de postagens feitas no *Twitter*, e se demonstra como é correlato ou até preditivo do índice *Down Jones* (BOLLEN et al., 2011, p. 6).

O estudo que afirmou essa possibilidade concluiu que as mudanças de opinião públicas podem ser rastreadas pelo conteúdo em larga escala de publicações de usuários do *Twitter*. Essa análise oferece uma complementação automática, rápida, gratuita e em larga escala a instrumentos tradicionais de predição do índice *Down Jones*, podendo inclusive ser otimizada para medir uma variedade de dimensões do Estado da opinião pública (BOLLEN et al., 2011, pag. 7).

Os dados assumem um papel tão importante na economia dentro do ambiente virtual que se converte na própria moeda. Como dito no item anterior deste capítulo, a riqueza está na informação. Os serviços na internet são prestados, na maioria dos casos, de forma gratuita. O custeio desses serviços é feito pelo fornecimento de dados pessoais, para viabilizar o direcionamento personalizado de conteúdo publicitário. Este, sim, irá custear o bem consumido no ambiente virtual (BIONI, 2019, p. 26).

Vivendo este momento do amplo uso dos dados pessoais, surge o questionamento sobre os reflexos jurídicos destes mercados. Primeira e evidentemente, o limite natural ao direito à informação é o direito à privacidade. Porém, não há lesão quando existe o consentimento, mesmo que implícito. É a hipótese em que a pessoa voluntariamente decide expor aspectos da própria vida. Da mesma forma, existem limites naturais ao direito de privacidade quando atinge interesses coletivos, momento em que tem de ser analisado caso a caso a predominância do interesse coletivo frente ao direito do particular.

Mesmo assim, é assegurado a todo o indivíduo o direito de proteção das suas propriedades, bem como o da sua privacidade. O ambiente digital não muda isso. Fala-se em propriedades, pois elas podem ser tanto bens tangíveis como intangíveis. Em se tratando informação como riqueza, estas são um ativo, em última análise, sendo assim propriedade do indivíduo e merecedor de proteção. O questionamento trazido por Patrica Peck Pinheiro (2013, p. 52) é se a sociedade digital caminha neste sentido, da proteção, ou se caminha no sentido oposto, da liberalização.

A mesma autora continua o questionando sobre o que pode ser feito com os dados coletados. Houve um movimento inicial em que as empresas inseriram em suas políticas de privacidade a garantia de uma maior propriedade dos dados para elas, justificando ser sua moeda de troca pelos serviços, como já foi dito. Porém, até onde essa relação é justa e proporcional? O exemplo dado é se um usuário destaca em seu perfil o *hobby* de jogar tênis dá ou não o direito a uma empresa de usar isso para abordá-lo, ainda que para oferecer uma raquete de brinde ou vender uma assinatura de um clube do esporte. Para a autora, se o indivíduo determinou a informação com pública e a coleta foi de forma legítima, então, o uso está dentro de um propósito razoável, pode ser chamado de justo (PINHEIRO, 2013, p. 52). Por isso a importância de as legislações desenharem os limites desse direito, para definir até onde a forma é legítima e o propósito é razoável.

A autora prossegue afirmando que o indivíduo deve sempre deter sempre o direito de pedir para que a empresa lhe contate por este canal. Se o número do celular de um indivíduo está disponível, a empresa pode lhe contatar por ele, tendo o indivíduo o direito de pedir que não utilizem este meio. Entende a autora citada que fica razoável para ambas as partes, já que o usuário tem o direito de não passar seus dados, bem como de não querer que uma empresa utilize a informação, da mesma forma que a empresa tem o direito de não o querer como seu cliente. Se o usuário não concorda com os termos de serviço, simplesmente não segue a diante (PINHEIRO, 2013, p. 52).

A criação da economia informacional cria um sistema socioeconômico distinto daquele presente na revolução industrial. O atual momento tecnológico modifica o escopo e a dinâmica da economia existente da era industrial. Cria uma economia global e promove uma nova onda de concorrência entre os agentes econômicos tradicionais e os novos atores naturais da era da informação. A nova realidade

econômica baseada em conhecimentos para toda a esfera de processos econômicos globais requer transformações sociais, culturais e institucionais básicas.

Assim, a econômica é informacional, pois os atributos culturais e institucionais de toda a sociedade são incluídos no novo paradigma tecnológico (CASTELLS, 2011, p. 141). Vê-se como a previsão do professor Manuel Castells se concretizou quando observamos os atuais hábitos de consumo, o quanto a sociedade foi modificada em sua cultura e comportamento pelo surgimento das tecnologias e dos mercados baseados em dados e como o comportamento humano foi modificado desde o surgimento da internet até os dias de hoje. Porém, o autor complementa dizendo que o que mudou não foram as atividades em que os seres humanos estão envolvidos, somente sua capacidade superior em processar símbolos (CASTELLS, 2011, p. 142).

Essa economia informacional é também global. Recebe identificação como global por ter capacidade de funcionar em tempo real, como unidade, em todo o planeta. Tornou-se assim com base na nova infraestrutura proporcionada pelas tecnologias da informação e da comunicação. As economias de todo o mundo dependem do desempenho de um núcleo globalizado. Nesse núcleo, estão o mercado financeiro, o comércio internacional, a produção transnacional, a ciência e tecnologia e a mão de obra especializada. Assim, define economia global como uma em que seus componentes centrais têm capacidade institucional, organizacional e tecnológica de trabalhar em unidade e em tempo real em escala global (CASTELLS, 2011, p. 143).

Vê-se que os elementos-chave para a economia informacional baseiam-se na geração de conhecimentos e no processamento de dados. Essas são as ferramentas fundamentais para a concorrência entre as empresas (CASTELL, 2011, p. 165).

Podemos constatar que uma nova economia emergiu no final do Século XX e apresentou novas grandes empresas pelo mundo. Suas características são informacionais, interconectivas e globais. Assim, a Sociedade Digital do Século XXI tem como seu principal veículo a internet (FREIRE E ALMEIDA, 2015, p. 373).

Igualmente, vivemos hoje em dia uma economia com base na observação constante do comportamento das pessoas online. Uma economia com base na vigilância. Suas informações são tratadas como a matéria-prima explorada para gerar riqueza. Existe uma complexa rede de organizações que fazem negócios com base nessas informações pessoais dos consumidores, negociando-as entre si. Agem de em conjunto, cooperativamente, para agregar cada vez mais dados dos usuários e

tornar a mensagem publicitária, a propaganda política ou o simples consumo cada vez mais eficiente (BIONI, 2019, p. 49).

Com o atual desenvolvimento de legislações que dificultam o processamento de dados, está em curso uma mudança nessa economia. As empresas estão sendo forçadas a buscar novas formas de se conseguir dados dos seus consumidores. Não unicamente pela maior rigorosidade regulatória, mas porque as principais companhias que detêm esses dados, em especial o *Google*, *Facebook*, *Microsoft* e *Amazon*, estão menos dispostas a compartilhar os dados que possuem. Essas companhias reduziram a quantidade e os tipos de dados armazenados que eles estão dispostos a fornecer no mercado, o que irá afetar outras empresas que dependem desses dados (JURCYS et al., 2020, p. 3). Isso importa em um maior controle da economia por esses mesmos gigantes.

Outra inovação que está criando situações nesse mercado é a maior proximidade do dado do indivíduo. Um dado centralizado em um banco logo se desatualiza. Porém, ao se conseguir esses dados direto do aparelho do indivíduo ou em das contas de dados na nuvem do indivíduo, isso garante a atualização da informação e reduz o custo e o risco da coleta de dados, com o consentimento do consumidor. Dessa forma, essas empresas deixam de depender de dados desses bancos centralizados e permite que os serviços ofereçam ao consumidor uma experiência mais personalizada.

Além disso, também tem grande consequência na ciência de dados. Como os aplicativos de dados mais avançados exigem uma maior profundidade e amplitude de dados, as mais avançadas posições em ciência de dados estão com quem os possuem, em geral com a própria plataforma de dados ou com informações de agências governamentais, como, por exemplo, a Agência de Segurança Nacional dos Estados Unidos. A consequência natural é o interesse profissional está ligada a essas instituições (JURCYS et al., 2020, p. 4).

Em geral, percebe-se que, na era da internet, as pessoas comuns estão se tornando extraordinariamente vulneráveis, por tomar parte da economia e da sociedade digital onde frequentemente envolve revelar informações pessoais para organizações gigantes que facilmente conseguem armazená-las, processá-las, compartilhá-las sem que o indivíduo tenha uma opinião ou sequer o conhecimento disto (DIXON, 2018, p. 29).

Portanto, conclui-se que existe vigente não só uma economia informacional, que já era global por natureza. A internet e as suas superfirmas criaram um sistema de economia baseado na utilização, transformando os dados e as informações coletadas em verdadeira riqueza no mundo real. Essas empresas atuam no mundo todo e detêm consumidores no mundo todo. Mais importante, operam esses dados, levando-os de um local a outro no globo de forma instantânea, sem a pressão legislativa recente, sem se importar com a privacidade ou os direitos de resguardo do cidadão sujeito desse dado.

A transferência internacional de dados e sua utilização como fonte giradora de riquezas é, em conclusão, o ponto central dessa economia global baseada em vigilância. O trabalho tenta demonstrar uma hipótese em que esse mercado não deixa de existir. Seus benefícios são reais e é um progresso importante no sentido de reduzir ainda mais as fronteiras do mundo. Leva isso em consideração para criar um instrumento que permita que o usuário esteja inserido nesse mercado de uma forma menos vulnerável.

3 A INTERNET COMO GERADORA DE CONFLITOS ENTRE JURISDIÇÕES

Já foi demonstrado como os dados e a informação, de modo geral, são a riqueza da sociedade digital. É a fonte de lucro das empresas que atuam na internet. Essas empresas são gigantes, afetando um número infindável de pessoas em todo mundo. Mais da metade das pessoas no mundo utilizam internet diariamente, compartilhando seus dados com essas organizações, que os compartilham entre si. Porém, o direito evolui dentro do ambiente digital para proteger o indivíduo, notadamente o direito do usuário sujeito à exploração de seus dados. É o direito à proteção de dados pessoais. Porém, como espalhar esse direito de forma global, sem sucumbir para a criação de uma arquitetura da internet cheia de fronteiras estatais?

Este capítulo tem por objetivo demonstrar exemplos de conflitos que envolvem a internet como propulsora de dificuldades legislativas. Fatos jurídicos nunca conhecidos que vieram a existir por conta do avanço tecnológico e da ciência de dados, suas repercussões internacionais, seja no conflito direto entre jurisdições, seja nas relações internacionais. Isso para justificar uma solução que venha a ser global de governança para a internet. Não se trata apenas da falta de legislação própria para a internet global, mas a falta de sistemas de governança que consigam apoiar as nações diante dos problemas aqui elencados.

Desde que se iniciou o debate de aplicação do direito para questões que envolvem a internet, sempre ficou clara a máxima de que mesmo que a internet permita um alcance geograficamente disperso, ela não modifica a responsabilidade de seus atores dentro das fronteiras nacionais (REIDENBERG, 2001, p. 4). Da mesma forma, a ONU já manifestou que qualquer direito que algum indivíduo possua *offline* também deve ser protegido online (ORGANIZAÇÕES DAS NAÇÕES UNIDAS, 2016, p. 3).

No entanto, quando tratamos da vigilância com um poder tão grande dentro da economia, vale lembrar que Lessig (2006, p. 23) questionou que tanto o monitoramento privado quanto o público, na era da sociedade digital, têm a característica destacável que podem aumentar, sem, contudo, alterar a carga sobre o indivíduo pesquisado, sem o conhecimento ou percepção do usuário. Assim, como que a proteção dada pelas legislações nacionais pode ser aplicada em um mundo que não imaginado pelos legisladores?

Agrava-se quando sabemos que os atores soberanos levam a sua soberania muito a sério, em especial quando se trata de ciberespaço. Cada um tem um senso de domínio próprio muito forte, às vezes, traduzindo esse domínio para além de seu próprio. Quanto mais a internet acolhe novos usuários, mais reivindicações de um soberano para controlar a expressão e o comportamento online entrarão em conflito com a reivindicação de outros soberanos. Para Lessig (2006, p. 279), esse conflito se provará o fato generativo mais importante para a internet.

O direito se preocupa em buscar a proteção de um direito que seja lesado. Por exemplo, se um consumidor chileno é lesado por um site brasileiro em uma relação de consumo, a lei aplicável é a lei do Chile. Se, por um acaso, não deseja se responsabilizar por problemas que ocorram no Chile, deve deixar seu limite de atuação claro. Deve informar quais usuários serão atendidos e qual legislação estará submetida, já que não necessariamente presença virtual, representa a possibilidade de poder ser acessado por indivíduos de qualquer parte do mundo. Assim, o princípio de proteção na sociedade da informação é a própria informação (PINHEIRO, 2013, p. 50).

Tanto o *Google* como o *Facebook* levam em consideração seu alcance global quando escrevem seus termos e serviços. Escolhem foro de eleição, ambas no Estado da Califórnia, nos Estados Unidos, porém, admitem a possibilidade de jurisdições nacionais de absorverem questões consumeristas para si. A cláusula redigida pelo *Facebook* é:

> Se você for um consumidor, as leis do país em que você reside serão aplicáveis a qualquer pleito, causa de ação ou contestação que você tiver contra nós decorrente de ou relacionada a estes Termos ou aos Produtos do Facebook (“reivindicação”), e você poderá resolver sua reivindicação em qualquer tribunal competente em tal país que tenha jurisdição para tanto. Em todos os outros casos, você concorda que a reivindicação deverá ser resolvida exclusivamente no tribunal distrital dos EUA no Distrito Norte da Califórnia ou em um tribunal estadual localizado no condado de San Mateo, que você se submeterá à jurisdição pessoal de qualquer desses tribunais para o fim de resolver esses pleitos e que as leis do estado da Califórnia regerão estes Termos e qualquer pleito, independentemente de disposições sobre conflitos de leis (FACEBOOK, 2018).

Da mesma forma, vemos nos termos do *Google*:

> Os tribunais de alguns países não aplicarão a lei da Califórnia a alguns tipos de disputas. Se você reside em um desses países, então, quando a legislação da Califórnia não puder ser aplicada, a legislação de seu país será aplicada às disputas relacionadas com estes termos. Nos outros casos, você concorda com a aplicação das leis da Califórnia, EUA, excluindo as normas da Califórnia sobre conflitos de leis, a quaisquer disputas decorrentes de ou relacionadas com estes termos ou Serviços. Da mesma forma, caso as leis em seu país não permitam que você concorde com a jurisdição e foro dos tribunais de Santa Clara, Califórnia, EUA, então jurisdição e foro locais serão aplicados às disputas relacionadas com estes termos. Nos outros casos todas as reclamações decorrentes de ou relacionadas com esses termos ou Serviços serão litigadas exclusivamente em tribunais estaduais ou federais da Comarca de Santa Clara, Califórnia, EUA e você e o Google autorizam a jurisdição pessoal nesses tribunais (GOOGLE, 2017).

Como vemos, ambos atraem a jurisdição para onde está localizada a sua sede, San Matteo e Santa Clara, Califórnia. Ao concordar com os termos, o usuário expressamente concorda em litigar com a legislação californiana para todos os casos em que não tenha previsão legislativa anterior que não permita a disposição de foro de eleição para o caso. Assim, percebemos como a natureza global da internet, além da sua arquitetura mundial, apresenta complexidades jurisdicionais para qualquer Estado exercer seu poder jurisdicional nacionalmente (FREIRE E ALMEIDA, 2015, p. 111).

Alguns casos são famosos e muito estudados demonstram como é difícil exercer o poder jurisdicional nacionalmente. O primeiro trazido como exemplo é o caso envolvendo *Yahoo!* e a França. Foi disponibilizado no *website* da *Yahoo!* a venda de itens com temática nazista. A legislação francesa proíbe a comercialização de produtos desta natureza. Porém, a legislação dos Estados Unidos não tem qualquer impeditivo. Então, o Estado francês ingressou com uma medida judicial dentro do judiciário francês para compelir a *Yahoo!* a remover da internet a venda de "memorabilia" nazista a usuários daquela nacionalidade (REIDENBERG, 2001, p. 2).

Dentro do poder judiciário francês, o Estado foi bem-sucedido e conseguiu uma ordem para que a *Yahoo!* não mais promovesse a venda desses itens a seus nacionais. Ocorre que a *Yahoo!* também ingressou com ação, agora perante a justiça americana, para impedir a eficácia da justiça francesa, que havia aplicado multa contra a empresa. Por ser uma organização com sede nos Estados Unidos, a alegação de que estava amparada pela primeira emenda da constituição americana em toda a sua ação na internet, mesmo que em caráter global, não podendo ser coagida a remover conteúdo do ar sob pena de aplicação de multa pela justiça francesa (REIDENBERG, 2001, p. 6).

Para o estudioso do direito na internet Joel R. Reidenberg (REIDENBERG, 2001, p. 6), este era apenas o argumento legal utilizado pela *Yahoo!* para não se submeter à jurisdição francesa na defesa de seus interesses. O que a empresa buscou foi proteger-se com a primeira emenda americana além das fronteiras daquela nação. A organização se recusou a cooperar com a justiça francesa esperando aplicar a primeira emenda em suas atividades globais. Para a primeira emenda americana, a *Yahoo!* tinha o direito de expressar ideias e políticas reprováveis. Porém, essa regra não se aplica a disseminação de *websites* na França com objetivo de atingir usuários franceses.

Portanto, essa pretensão da empresa americana de esconder-se na primeira emenda da constituição americana entra em choque com a jurisdição aplicada ao caso pela corte francesa. Apesar do conteúdo descrito ser legal dentro das fronteiras estadunidenses, na França, ela não é. A argumentação é de que, como a *Yahoo!* está localizada em território americano, a lei a qual ela deve observar em sua atuação é da americana para toda a internet (REIDENBERG, 2001, p. 6).

Como conclui o professor Joel R. Reidenberg (REIDENBERG, 2001, p. 7), a *Yahoo!* coletou o perfil de usuários franceses e direcionou sua publicidade a eles, em francês. Portanto, não pode alegar que buscou servir apenas o público americano e não o francês em sua atuação. A disponibilização daqueles itens com o espaço publicitário em francês para o público francês faz parte do modelo de negócios adotado pela *Yahoo!*, seja nos Estados Unidos ou na França.

No relato que o professor Reidenberg (REIDENBERG, 2001, p. 8) declara sobre o caso, o governo francês buscou forçar que a empresa americana respeitasse a lei de seu país enquanto realizava negócios em seu território. Ocorre que, ao sofrer o revés naquele país, a *Yahoo!* buscou o judiciário americano para negar a autoridade jurisdicional francesa. O autor ressalta que a intenção da *Yahoo!* parece tentar esconder sua real intenção, que é manter operante seu modelo de negócio, o que inclui vender os referidos itens mundo a fora, inclusive na França. O autor também menciona que a *Yahoo!* deturpa a decisão da corte do país europeu. Para a empresa, como não detém qualquer posse na França, apenas a justiça estadunidense poderia aplicar uma multa. Porém, o professor relembra que a Yahoo deixa de incluir que seus interesses e lucros em território francês são capazes de suportar qualquer multa. A alegação é de que a constituição dos Estados Unidos se aplica em todo o mundo, mas

o professor confirma que, mesmo em sentenças de cortes americanas, existem decisões similares àquelas adotadas pelo judiciário francês.

Outro caso em que está presente um conflito de jurisdição importante é o caso envolvendo a *Google* e o cidadão espanhol Costeja Gonzalez. A demanda versa sobre um pedido deste usuário que fosse desvinculado dos resultados de busca pelo seu nome a informação publicada em um jornal sobre um leilão de bens de devedores do fisco. Primeiramente, Gonzalez fez o requerimento para a agência de proteção de dados espanhola, que acolheu seu pedido e requereu que a empresa removesse da indexação o *link* para o leilão da pesquisa em nome de Gonzalez. Porém, tanto a *Google Inc.*, com sede nos Estados Unidos, como seu braço espanhol *Google Spain SL*, com sede em Madrid, promoveram uma medida judicial junto ao judiciário espanhol tentando reverter a decisão do órgão estatal. A justiça espanhola encaminhou o processo para o tribunal de justiça da União Europeia para analisar o caso à luz da diretiva 95/46/EC, a diretiva de proteção de dados à época em vigor (TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA, 2014).

Uma das alegações levantadas pelo *Google* é que como a *Google Inc.* é quem opera a ferramenta de busca e está situada nos Estados Unidos, não caberia aplicação da legislação europeia. Porém, quando o tribunal comunitário tratou da aplicação da possibilidade de julgamento do feito em jurisdição espanhola, analisou que a diretiva conferia a cada Estado membro o poder de aplicar suas disposições nacionais ao tratamento de dados pessoais quando for efetuado no contexto das atividades de um estabelecimento pelo tratamento estiver situado no território deste Estado membro, podendo inclusive o responsável pelo tratamento não estar estabelecido no território da comunidade (TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA, 2014).

São duas pessoas distintas, a *Google Inc.* e a *Google Spain*. A primeira é responsável pela ferramenta de busca conhecida como *Google Search*, enquanto a segunda é quem realiza a promoção de vendas de espaço publicitário direcionado à população espanhola. A atividade da *Google Spain* está diretamente ligada com a atividade da *Google Inc.*, já que o espaço publicitário só tem valor em razão da importância da ferramenta de buscas, bem como a *Google Search* só tem o poder de gerar lucro devido à venda de espaços publicitários (TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA, 2014).

Portanto, a corte europeia entendeu que a *Google Spain* é uma empresa subsidiária a *Google Inc.* em território espanhol, sendo um estabelecimento em território de Estado membro da União Europeia. O tribunal entendeu que o processamento de dados não se faz necessário que ocorra diretamente em território europeu. Requer apenas que o contexto de suas atividades esteja ligado para atrair a jurisdição para o Estado membro, sob o escopo da lei de proteção de dados daquele território (TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA, 2014).

Em suma, a conclusão do tribunal europeu não desistiu apenas sobre o direito ao esquecimento. Apreciou o escopo territorial da antiga diretiva de proteção de dados da União Europeia. A pergunta que foi feita à corte é até que ponto há o poder judiciário espanhol em aplicar os direitos de acesso e oposição contra empresa americana. Para o tribunal europeu, apesar da empresa sediada nos Estados Unidos, ela detinha um estabelecimento em Estado membro da União Europeia. Assim, está inserido no âmbito de aplicação particularmente amplo, extensivo para fora da União Europeia (ARGA E LIMA; CARVALHO, 2019, p. 59).

Também ocorreu um caso na justiça alemã, em que a Corte Federal de Justiça Alemã determinou a responsabilidade dos pais pelo pagamento da indenização, em razão de seus filhos menores terem feito *download* de conteúdo digital pirata relacionado a músicas da cantora Rihanna, usando um *site* de compartilhamento de música. A investigação levou até o IP de conexão que estava associado a um assinante da cidade de Hamburgo, pai dos menores. Este se defendeu perante o judiciário alegando que ele, assinante, não podia ser responsável pelo uso dos menores na internet doméstica familiar. Não foi o assinante quem cometeu o ato ilícito. A justiça alemã alegou que o responsável pela internet responde pelo uso da conexão, recaindo duplamente pelo pai ser responsável pelos atos do filho menor (PECK, 2018, p. 29).

Daniel Freire e Almeida (2019, p. 122), no artigo *O Poder da Internet e os Desafios da Internet Global* relaciona diversos casos que demonstram a dificuldade que os poderes judiciários nacionais enfrentam ao lidar com a internet.

O primeiro caso daqueles referidos pelo autor que iremos citar é o caso envolvendo *Bible & Gospel Trust x Wyman*. O caso ocorreu em 2005 e versou sobre difamação, violação de direitos autorais e interferências, em que a Corte Distrital de Minnesota - EUA optou por não exercer jurisdição em razão do *site* envolvido na

demanda estar localizado no Canadá. Segundo o autor, o tribunal encerra o caso ao analisar as normas jurídicas que determinam o exercício de sua jurisdição (FREIRE E ALMEIDA, 2019, p. 136).

Em outra decisão em que o juiz não conheceu do mérito é o caso que envolveu a empresa *Oxford Round Table Inc.*, localizada no Kentucky - EUA, na ação que moveu contra Sloan Mahone, uma professora associada da universidade de Oxford e cidadã inglesa. A demanda versou sobre críticas feitas em um *site* mantido por uma empresa de Washington - EUA e sobre uma série de e-mails enviados por Sloan a outros professores da universidade e mais uma pessoa em Illinois (FREIRE E ALMEIDA, 2019, p. 137). Este é um caso que demonstra como a internet é capaz de simultaneamente criar conflitos em várias localidades com um único fato.

Ao avaliar o fato de que, em ambos os casos, os tribunais encerraram as ações sem julgamento de mérito, o professor Daniel Freire e Almeida comenta que o ciberespaço torna fácil escapar impunimente, comparando com um fugitivo que escapa pelas fronteiras em um filme (FREIRE E ALMEIDA, 2019, p. 138).

Em sequência, o mesmo artigo chama a atenção ao caso em que a *Wikileaks* foi judicialmente acionada pelo banco *Julius Baer*, com sede na Suíça e nas ilhas Cayman, sobre documentos publicados pelo *site* em um tribunal californiano. A decisão ordenou o bloqueio do domínio e a remoção do site *wikileaks.com*. Ocorre que o conteúdo ainda se encontra disponível por outros endereços eletrônicos, em outros países. Assim, o autor conclui que esses casos são demonstrações de como a internet global desestabiliza as atividades judiciais dentro de limites geográficos (FREIRE E ALMEIDA, 2019, p. 139-140).

Em complemento, no mesmo artigo é trazido um caso envolvendo a empresa *Global Royalties* e *Xcentric Ventures*, no qual, após uma decisão de um tribunal canadense para remover declarações vexatórias de determinado *site*, um tribunal estadunidense se recusa a executar a decisão liminar em razão de ser oriundo de um tribunal estrangeiro. Para o autor, se tratou de desafio ao tribunal canadense que expediu a ordem (FREIRE E ALMEIDA, 2019, p. 144). Essa é uma demonstração, além dos obstáculos jurisdicionais para questões da internet, mas também da falta de cooperação entre os dois judiciários. O que leva o autor a questionar: *"*Qual é, então, a extensão do domínio jurídico de um país neste espaço virtual?*"* (FREIRE E ALMEIDA, 2019, p. 145).

Os casos da *Global Royalties* contra *Xcentric*, bem como o envolvendo o *Wikileaks*, revelam uma dificuldade em obtenção de eficácia nas decisões jurídicas nacionais frente à internet. Acrescenta-se a essa afirmação, trazidos pelo professor Daniel Freire e Almeida (2019, p. 160), no mesmo artigo, mais dois casos de carta rogatória ao Brasil.

O primeiro caso, originário do tribunal da comarca de Düsseldorf, na Alemanha, para a companhia *UOL – Universo Online*, o qual o Superior Tribunal de Justiça brasileiro levou mais de um ano e meio para despachar (FREIRE E ALMEIDA, 2019, p. 160). Da mesma forma, uma carta rogatória de Bolonha, Itália, contra *Terra Networks Brasil S.A.* acabou por esperar quase dois anos para ser despachada. Quando o foi, a empresa brasileira alegou não ter tecnologia necessária para atender o juízo em identificar o usuário pelo seu IP (FREIRE E ALMEIDA, 2019, p. 161). Seja pelo decurso do tempo, pela incapacidade técnica, sua velocidade de disseminação ou por questões tecnológicas, a internet compromete os mecanismos tradicionais de justiça.

Este capítulo e a apresentação destes casos têm por objetivo demonstrar a necessidade de uma solução internacional quando falamos da internet. Trata-se de um ambiente que requer uma solução internacional.

No mesmo sentido, Daniel Freire e Almeida (2019, p. 174) conclui em seu artigo que, quanto mais pessoas estão conectadas, mais conflitos ou conveniências existiram entre os poderes soberanos, com Estados nacionais aceitando ou negando exercer sua jurisdição de acordo com interesses. Ao mesmo tempo, acerta a necessidade de aperfeiçoar os mecanismos de cooperação internacional, lentes demais para a internet. O autor entende como necessário um novo plano a nível internacional e harmonizado, na direção de uma judicialização internacional, mais apropriada para o ambiente digital.

O mesmo autor apresenta, em outro trabalho, uma solução para estas dificuldades. Ele fala sobre a hipótese de um Tribunal Internacional para a Internet como a melhor técnica jurídico-internacional para a resolução desses conflitos de direito internacional na internet. Esse tribunal teria os contornos de uma organização internacional focada no julgamento de conflitos internacionais da internet e comércio eletrônico, com personalidade jurídica internacional necessária para cumprir seu papel

e jurisdição universal, abrangendo indivíduos, sociedades, Estados e organizações internacionais (FREIRE E ALMEIDA, 2015, p. 381).

O presente trabalho apresenta hipótese semelhante, uma organização internacional também com fulcro em possibilitar uma maior cooperação internacional entre jurisdições, bem como uma forma de lidar com os dados que navegam o mundo em segundos de uma forma global. Assim, superam-se as dificuldades jurisdicionais que as nações soberanas podem enfrentar ao se fazer valer suas leis de proteção de dados, bem como dar assistência aos usuários de países em que essas leis não existem.

Um dos conflitos indispensáveis a serem falados em se tratando de internet global e proteção de dados pessoais é o caso envolvendo o ex-agente de inteligência dos Estados Unidos Edward Snowden. Em 2013, o funcionário da *National Security Agency* (NSA) tornou público o maior esquema conhecido de espionagem e de vigilância de indivíduos. O esquema utilizado pelo governo estadunidense filtrava dados coletados de serviços das gigantes empresas que operam na internet, como *Apple*, *Facebook*, *Google* e *Microsoft* (LOPES, 2015, p. 262).

O caso expõe a espionagem de dados de brasileiros, incluindo da presidente do Brasil à época, Dilma Rousseff, mesmo sem nenhuma relação com terrorismo. A espionagem estaria acontecendo interceptando dados dos cabos submarinos que cortam o litoral brasileiro. Com base no que foi divulgado tanto por Snowden, quanto pelo jornalista responsável pela divulgação dessas informações, Gleen Greenwald, além de outros documentos antigos vazados pela *Wikileaks*, a cidade de Fortaleza é um *hub* de fibras ópticas que distribui dados por todo o mundo. Razão pela qual há o interesse em espionagem nessa região (LOPES, 2015, p. 264).

Para detalhar melhor as acusações feitas por Snowden, o ex-agente alega ter descoberto a captura maciça de e-mails e chamadas telefônicas por agentes de inteligência do governo dos Estados Unidos. Diariamente, cerca de 550 analistas eram destacados para avaliar os dados captados. Tais acusações também implicariam o governo alemão e de outras nações ocidentais.

Nas acusações feitas ao jornal *The Guardian,* os agentes de inteligência podem encontrar no banco de dados da NSA os nomes, endereços de e-mail, senhas, números de telefone e palavras-chave sem precisar de aprovação de um juiz em tempo real a atividade de qualquer indivíduo. Isso significa dizer que o governo

americano tinha acesso irrestrito à internet e telefone de qualquer pessoa, exercendo vigilância total de todas as atividades diárias de qualquer cidadão de qualquer país por meio da internet, incluindo operações bancárias, compras em cartão de crédito, conversas. A acusação é de que o governo americano consegue acessar quase tudo o que um usuário da internet faz, como e-mails, pesquisas e dados de milhões de pessoas (VERNIK, 2014, p. 102-103).

Cabe destacar a reação das revelações nos países latino-americanos. O Itamaraty fez um pedido de explicações dos Estados Unidos a respeito da espionagem de cidadãos brasileiros pela NSA. Na Argentina, a presidente Cistina Kirchner demonstrou interesse em uma denúncia feita pelo Mercado Comum do Sul (Mercosul). O presidente do Peru na época dos fatos, Ollanta Humala, pediu investigação do congresso de seu país. O então vice-presidente do Equador, Jorge Glas, declarou como inaceitáveis os atos de espionagem, também requerendo explicações, exigindo transparência a respeito das normas internacionais e ao marco jurídico que protege a privacidade e as telecomunicações (VERNIK, 2014, p. 108).

Em se tratando da Bolívia, ocorreram repercussões e desdobramentos bastante diferentes. Havia suspeita de que Edward Snowden, naquele momento, já procurado pela polícia dos Estados Unidos, pudesse estar à bordo do avião presidencial, o que acarretou detenção do presidente em Viena. A aeronave trafegava no espaço aéreo europeu sem que quatro países da região lhe dessem autorização. O evento foi descrito como uma grave ofensa a Morales e ao país.

Imediatamente, solicitaram uma reunião de emergência da União das Nações Sul-americanas (Unasul). Os governos boliviano e venezuelano acusaram os Estados Unidos de terem orquestrado o pouso forçado do avião em Viena. O presidente Morales afirmou nunca ter encontrado Snowden em Moscou, que foi para onde o ex-agente fugiu das autoridades americanas. O governo boliviano chegou a denunciar os EUA na ONU (VERNIK, 2014, p. 103-104).

Os presidentes da Unasul, estando presentes Brasil, Argentina, Equador, Venezuela, Uruguai e do Suriname, além de representantes de povos indígenas ligados a Evo Morales, se reuniram para expressar rejeição imediata ao evento, dito ser capaz de criar precedente perigoso de direito internacional. O evento acarretou também pedido de explicações da Bolívia aos embaixadores de Espanha, França, Itália e Portugal (VERNIK, 2014, p. 106-107).

Por fim, em nova reunião da cúpula do Mercosul, os presidentes de Uruguai, Argentina, Venezuela e o próprio Evo Morales se encontraram mais uma vez. Segundo o presidente boliviano, o governo americano estaria lendo os e-mails de grandes autoridades bolivianas. A Argentina repetiu a declaração em relação aos seus cidadãos. Morales afirmou que os EUA gastam, todos os anos, mais de setenta e cinco milhões de dólares para manter a vigilância. Além disso, a cúpula decidiu consultar embaixadores presentes nos quatro países que detiveram o avião de Evo Morales, além de criticar os EUA pelo desenvolvimento do esquema global de espionagem (VERNIK, 2014, p. 109).

Além da repercussão dentro do cenário da política sul-americana, também cabe ressaltar as consequências do caso para a própria população dos Estados Unidos. Primeiro, destaca-se as reações de atores sociais, por meio de organizações não governamentais de defesa dos direitos e liberdades civis, em destaque a *Eletronic Liberties Union,* que manifestou repúdio às medidas adotadas pela NSA.

Também foi apresentado o manifesto intitulado *Global Government Survillance Reform,* no qual as maiores empresas de tecnologia do mundo (*AOL*, *Apple*, *Facebook*, *Google*, *Linkedin*, *Microsoft*, *Twitter* e *Yahoo!*), sugerem um novo modelo para a coleta e tratamento de dados dos usuários da internet. Esse documento apresentou cinco princípios fundamentais, limitação da coleta de informações de usuários pelos governos, fiscalização e prestação de contas, transparência sobre exigências governamentais, respeito ao livre fluxo de informações e evitar conflitos entre governos. Além disso, foi constituída uma coalisão legislativa para criar legislações que visam bloquear ou até anular as ações da NSA (BOFF; FORTES, 2016, p. 351-352).

O caso de Snowden é importante uma vez que não envolve a internet em escala global. Envolve a internet como criadora de conflitos não só jurídicos, como um complexo conflito internacional, implicando diversas nações, esse conflito internacional sendo provocado pela vigilância do governo americano de dados pessoais coletados de diversas fontes e incluindo as grandes empresas da internet. Assim, é um caso que evidencia de forma contundente uma necessidade para uma solução global para a proteção de dados pessoais. ,

A acusação é da interferência da NSA não só na privacidade de cada indivíduo que utiliza a internet, mas também de governos e autoridades de primeiro escalão. É

uma acusação gravíssima que acabou por gerar um conflito internacional considerável e até a detenção de um presidente em território estrangeiro. Foi um fato de primeira grandeza para o direito internacional, para o direito na internet e as relações internacionais.

A repercussão do caso no Brasil pode ser vista inclusive na adoção de medidas legislativas em relação à internet. Um exemplo é o Marco Civil da Internet e da Lei de Crimes Informáticos, que mantém grande proximidade à compreensão jurídica da internet e dos efeitos que possui na vida dos indivíduos e da sociedade. Essas leis representam uma resposta sobre os efeitos gerados pela repercussão do caso do esquema de vigilância em massa da NSA. O tema à época não foi esgotado por essas legislações, sendo necessária a Lei Geral de Proteção de Dados Pessoais, que viria apenas anos depois (BOFF; FORTES, 2016, p. 363).

O caso de Snowden balançou com muita força o entendimento de como os dados são usados na internet. Escancarou ao mundo a capacidade de vigilância que a internet pode conferir, seja para entidades governamentais, como também para as gigantes da internet. Essas empresas se manifestam em repúdio à utilização dos dados pelo governo, mas seguem se utilizando deles como sua maior fonte de riqueza. Assim, vivemos dentro desta estrutura que favorece a vigilância, sem que sequer o usuário saiba de tudo o que se sabe sobre ele.

O caso que é de grande conhecimento geral e elevou as preocupações de todos com o assunto de proteção de dados é a utilização pela *Cambridge Analytica* dos dados de 87 milhões de pessoas, extraídos do *Facebook*, a serviço da campanha eleitoral de Donald Trump para a presidência dos Estados Unidos em 2016. A empresa conseguiu acessar um grande número de dados de usuários da rede social por meio de um teste psicológico que era frequentemente compartilhado no site (G1, 2018).

As informações eram coletadas por um aplicativo chamado *thisisyourdigital life*, um teste em que quem concordasse em fazer recebia uma pequena quantia de dinheiro e teria seus dados coletados para fins acadêmicos. O aplicativo se aproveitou de uma falha nos termos do *Facebook* para ter acesso a nome, profissão e moradia, gostos, hábitos e redes de contato, e entregou à campanha de Donald Trump. Os dados foram usados para catalogar o perfil das pessoas e direcionar, de forma

personalizada, mensagens em prol do candidato eleito naquela eleição e contrários à candidata derrotada, Hilary Clinton (BBC, 2018).

O último caso que esse trabalho apresenta para reflexão é o mais recente envolvendo o *Facebook* e Gambia. Esse caso simboliza muito a importância de uma solução global e que determine princípios para uma transparência global dos dados processados. Gambia é um país com menor poder de influência global e sem a proteção adequada para a proteção de dados. Ele entrou com um processo requisitando informações do *Facebook* junto à justiça americana para que a empresa forneça dados sobre contas suspensas ou excluídas que servirão como prova em litígio na Corte Internacional de Justiça envolvendo Gambia e Myanmar por cometimento de genocídio.

O *Facebook* baniu de sua plataforma militares de Myanmar responsáveis por promover sérias violações de direitos humanos e propagação de discurso de ódio contra a população Rohingya. Assim, Gambia pede na justiça americana documentos e comunicações que foram criadas e publicadas por uma lista de indivíduos e organizações de Myanmar, como o Comandante-Chefe General Min Aung Hlaing, a polícia de Myanmar, a 33ª e a 99ª divisão de infantaria leve de Myanmar, além de outros elementos que podem ter ligação com a violação de direitos humanos. Também é pedido que ao *Facebook* documentos de qualquer investigação interna de violação de conteúdo feita pela empresa das pessoas marcadas na lista (DOMINO, 2020).

Esse caso desenha bem a importância de uma solução global. A falta de transparência ou a recusa em fornecer esses dados por parte do *Facebook* pode privilegiar pessoas que estão sendo investigadas por genocídio. O direito à investigação de um crime de genocídio não pode ser obstaculizado por um direito de privacidade daquele que cometeu o crime. Uma organização internacional aqui poderia ser o intermediador desses dados. Bem como acervar a situação e definir se o caso merece a entrega ou não dos dados.

4 A PROTEÇÃO DE DADOS PESSOAIS VISTA COMO UM DIREITO DA PERSONALIDADE

O presente capítulo tem por objetivo demonstrar a evolução do direito de proteção de dados pessoais como um direito da personalidade. Tenta-se criar a diferenciação deste direito de outros direitos conexos, como o da privacidade. A relevância disso para o tema é que, por se tratar de um direito da personalidade, este é ligado a todo e qualquer ser humano. Assim, é um direito que merece ser atendido a todas as pessoas, em todos os lugares. É insuficiente, portanto, apenas a criação de algumas leis nacionais para a promoção desse direito. O escopo deste capítulo é baseado na comprovação de que este é um direito que deve estar presente em todos os lugares, se não de forma uniforme, de modo muito semelhante, bem como é o objetivo de outros direitos humanos.

Primeiramente, conceitua-se a proteção de dados pessoais. Trata-se da legislação desenvolvida com o intuito de proteger os seus dados pessoais. Na sociedade atual, para se entregar o controle de seus próprios dados aos indivíduos, é fundamental a existência de leis de proteção que restrinjam e moldem as ações de governos e companhias. Sem qualquer legislação a respeito, essas organizações mostram repetidamente que irão coletar tudo o que puderem, garimpar tudo, manter pelo tempo que bem desejarem, compartilhar com quem quiser, sem que o indivíduo tenha conhecimento, a menos que legislações sejam eficazes em restringi-las (PRIVACY INTERNATIONAL, 2018, p. 3).

Assim, as legislações concedem o acesso aos dados direitos perante às empresas, relacionadas aos dados que essas empresas possuem coletados sobre eles. O acesso é dado pelo direito de obter informações sobre os quais são coletados ou processados, ou ainda o direito de conseguir cópias digitais dos dados processados. Esses direitos, geralmente, são complementados com outros direitos, como o de solicitar a exclusão da venda destes dados (JURCYS et al., 2020, p. 8).

Já a carta dos direitos fundamentais da União Europeia, em seu artigo 8º, determina que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. Além disso, determina que esses dados devem obrigatoriamente ser objeto do que o texto configura como um tratamento leal, com finalidade específica e com o consentimento do indivíduo ao qual se refere o dado.

Também dá a todos o direito de conhecer os dados coletados sobre si e a requerer correções daqueles que não estão corretos. O direito da privacidade está posto no artigo 7º da carta. Isso serve para demonstrar a evolução da proteção de dados como um direito por si.

Da mesma forma, a *General Data Protection Regulation* tem uma missão muito audaciosa de moldar parte importante da vida contemporânea. Como nossa sociedade cada vez mais se vê dependente de da tecnologia digital, a proteção de dados não é um luxo, define expressamente a legislação como um direito fundamental (DIXON, 2018, p. 28). Isso porque, na internet, os indivíduos estão cada vez mais vulneráveis. Isso se dá já que participar da atual sociedade e da economia com base na coleta de dados envolve revelar grandes quantidades de dados que podem ser coletados, armazenados, processados e compartilhados sem qualquer participação do sujeito (DIXON, 2018, p. 29).

O supracitado é reforçado pelo posicionamento de Bruno Ricardo Bioni, que relembra que a proteção de dados não está limitada ao debate entre público e do privado. Assim, torna-se diferente do direito à privacidade. Para o autor, tratar como uma evolução unicamente relacionada com o direito à privacidade seria uma construção dogmática falha. É o autor que constata o direito à proteção de dados como um novo direito da personalidade que angaria autonomia própria (BIONI, 2019, p. 99).

Já a Lei Geral de Proteção de Dados brasileira, número 13.709/18, em seu artigo 1º, diz que a legislação dispõe sobre o tratamento de dados pessoais, sendo estes digitais ou não, por pessoas naturais ou jurídicas, de direito público ou privadas, com o objetivo de proteger os direitos fundamentais de liberdade e privacidade, além do livre desenvolvimento da pessoa natural. No artigo 2º, dispõe-se como princípio o respeito à privacidade, à autodeterminação informativa, à liberdade de expressão, à inviolabilidade da honra e da imagem, ao desenvolvimento econômico e tecnológico, aos direitos do consumidor, direitos humanos e da personalidade, dignidade e ao exercício da cidadania.

O referido artigo da legislação brasileira ainda guarda clara relação do direito de proteção de dados com o de privacidade. Isso porque por mais que seja um novo direito que tenha surgido, ainda guarda grande similaridade.

Ambos os direitos estão intrinsicamente ligados. Os usuários da rede, como cidadãos ou consumidores, precisam deter de ferramentas e mecanismos para defender sua privacidade e se proteger dos abusos no processamento de dados. Também é importante uma definição clara das obrigações daqueles que processam os dados, para que seja possível a tomada de posturas que permita o usuário a defender-se desses abusos, atenuando-se, assim, os prejuízos ao seu direito à privacidade e seja capaz de se responsabilizar aqueles que não cumprem essas obrigações. A proteção de dados pessoais significa proteger a privacidade regulando o processamento das informações coletadas, fornecendo, assim, o direito sobre os dados ao indivíduo ao qual ele se refere e estabelecendo um sistema de responsabilidade e obrigações claras para aqueles que controlam ou realizam o processamento de dados (PRIVACY INTERNATIONAL, 2018, p. 12).

Porém, o direito brasileiro admite também outros embriões para a proteção de dados pessoais, muito anteriores ao advento da internet. Está consagrado na Constituição Federal de 1988, em seu artigo 5º, inciso LXXII, o instituto do *Habeas Data*. Este direito assegura ao cidadão brasileiro o direito fundamental de conhecimento de informações relativas à sua pessoa, constante de registros ou banco de dados de entidades governamentais ou de caráter público. Além disso, dá direito ao indivíduo de solicitar, por processo sigiloso, jurídico ou administrativo, a correção dessas informações. A constituição é anterior ao amplo uso da internet, ou pelo massivo uso dos dados em entes privados que estão inseridos em ambiente digital, porém, já é possível notar semelhanças entre o remédio constitucional do *Habeas Data* e o que hoje se entende por proteção de dados pessoais.

No Código de Defesa do Consumidor, já em matéria infraconstitucional, vê-se a obrigação de se garantir acesso ao consumidor das informações que sobre ele constem em cadastros, fichas, registros, e dados pessoais ou de consumo que o fornecedor detenha sobre ele em seus arquivos, bem como também suas respectivas fontes (artigo 43). Isso constitui, inclusive, em infração ao direito do consumidor e penal em caso de impedir acesso ao consumidor a esses dados ou deixar de corrigir as informações que constam no cadastro.

Ademais, a publicação *The Keys to Data Protection: a guide for policy engagement on data protection* traz o exemplo do artigo 15 da Constituição Colombiana. Este disposto, conforme emenda datada de 1995, instituiu a todos os

indivíduos colombianos o direito de saber, atualizar e retificar informações coletadas sobre ele em bancos de dados. Muito importante destacar que o alcance do referido dispositivo é de registros de entidades públicas ou privadas (PRIVACY INTERNATIONAL, 2018, p. 13).

É nesse ponto em que se observa a grande diferenciação que existe entre o direito de proteção de dados pessoais e a simples defesa da privacidade. Quando se fala na defesa da privacidade, está sendo debatido o direito daquele indivíduo de ver suas informações protegidas e o consentimento que ele pode ter sobre expor esses dados a quem deseja processar ou não.

Porém, mesmo o *Habeas Data*, brasileiro ou colombiano, ou a defesa do consumidor no artigo 46 da lei 8.078/90, bem como as modernas leis de proteção de dados pessoais defendem o direito ao indivíduo de pleitear a modificação de determinados dados que não estejam corretos ou adequados. Não se está visando promover que determinada informação esteja reservada apenas ao âmbito privado. Não se questiona o interesse público daquela informação ao indivíduo, apenas requer que este esteja correto, atual ou adequado. É nesse momento que a proteção de dados pessoais se divorcia do direito à privacidade e ganha vida e proteção própria e independente.

Passa-se, então, a argumentar o direito de proteção de dados pessoais, não somente como um direito em si, mas como um direito da personalidade. Para Maria Helena Diniz, trata-se de direito da personalidade como o direito do indivíduo de proteger aquilo que lhe é próprio, como a identidade, a honra, a sociabilidade, entre outros. São direitos comuns da existência, são simples permissões da norma jurídica a cada pessoa de defender um bem que lhe é entregue pela própria natureza. São direitos subjetivos de exigir um comportamento negativo dos outros, protegendo um bem inato (DINIZ, 2004, p. 120).

Reforça o conceito de direito da personalidade dizendo que este se apoia na ideia de que, diferenciando dos direitos que podem ser apreciados economicamente, como o direito da propriedade ou o direito de crédito contra um devedor, existem outros direitos a serem considerados, que não perdem em valor, merecedores de proteção legal, que são inerentes à pessoa humana e estão ligados ao indivíduo de maneira perpétua e permanente. São inalienáveis e sua existência tem sido proclamada pelo direito natural (GONÇALVES, 2013, p. 156).

Desses, se dividem em duas categorias distintas, os inatos ou adquiridos, que decorrem de um *status* individual e existem na extensão da disciplina, conferidos pela legislação. Os primeiros têm como exemplo o direito à vida ou a honra, e os segundos têm como exemplo o direito autoral (GONÇALVES, 2013, p. 157). Assim, conclui-se que o direito de proteção de dados pessoais tem essa característica de inato ao indivíduo, seja por um direito natural, ou pelo direito legislado como fundamental, nas constituições nacionais, ou infraconstitucionais para uma visão mais positivista.

Da mesma forma, o direito de proteção de dados pessoais aparece na carta fundamental de direitos fundamentais da União Europeia como um direito nato a todo cidadão. Igualmente é o *Habeas Data* na constituição brasileira. Assim, por se tratar de um direito que está diretamente correlacionado com privacidade, imagem, honra, liberdade, entre outros, é que se deve entendê-lo como um direito da personalidade. Mais que isso, deve também se entender como um direito humano, sendo considerado com este nome, ou de forma embrionária, como fundamental em diversas constituições.

Assim, os dados pessoais representam contextos sociais importantes. Por essa razão, sua proteção está inserida na gama de direitos da personalidade, configurando como um direito fundamental autônomo. Portanto, a proteção de dados pessoais implica também em uma proteção ampla da privacidade, para além de não ter seu espaço pessoal invadido, hoje o indivíduo é carecedor de poder sobre suas informações pessoais. Assim, requer transparência de como seus dados podem ser utilizados por entes públicos e privados e um protagonismo maior do usuário (COSTA; OLIVEIRA, 2019, p. 38).

Porém, falando-se na economia com base na vigilância, a sociedade já evoluiu para entender a construção em que o público e o privado andam lado a lado para contribuir com para pagar a conta dos serviços online, que é a razão da importância das legislações de proteção de dados pessoais como uma consolidação de regras de conduta para quem processa dados online. Afirma-se, cada vez mais, a necessidade de transparência por parte das empresas da internet para que fique claro quais os dados estão sendo processados, por quanto tempo e com qual finalidade. Questiona-se se estamos dispostos a renunciar serviços prestados de forma gratuita online, as redes sociais, em troca da completa proteção dos nossos dados.

Para a autora Patrícia Peck (PINHEIRO, 2013, p. 56), a resposta é *não*, por mais que os indivíduos tenham interesse de sentir controle sobre os próprios dados, e que o Direito os proteja contra abusos, por mais que nós mesmos que tenhamos, de livre e espontânea vontade, disponibilizado esses dados a esses terceiros. Seja no momento do cadastro, seja pelo o que é postado em redes sociais. A autora afirma que vencerá o mercado quem estiver na vanguarda da proteção de uma privacidade sustentável, com transparência. Qualquer formato que implique ou no extremo de total liberdade, ou na proteção irrestrita, está fadado ao fracasso.

Por fim, conclui-se que qualquer tentativa de regular a proteção de dados pessoais é de vital importância que leve em conta a existência dessa economia com base em vigilância. O que proporciona a ocorrência de estratégias regulatórias complementares que, ao mesmo tempo em que representam um importante empoderamento do indivíduo para exercer um controle significativo sobre os seus dados pessoais, também revelam a consideração de o próprio fluxo das informações pessoais não deve submeter-se, apenas à lógica dos interesses econômicos em jogo (BIONI, 2019. p. 50).

Assim, aparece como de suma relevância as características da internet debatidas anteriormente nessa dissertação para encontrar o balanço entre a liberdade e os benefícios que a economia com base nos dados nos proporciona, em choque com aquilo que os indivíduos desejam e merecem que seja protegido.

5 AS LEIS DE PROTEÇÃO DE DADOS E COMO ELAS TENTAM ABRANGER AS PESSOAS NA INTERNET GLOBAL

O atual capítulo pretende buscar uma reflexão sobre as tentativas das legislações nacionais em encontrar uma solução para lidar com a presença global na internet. São definições legais que restringem o processamento de dado internacional ou definem responsabilidade de forma territorial sobre dados que trafegam de forma transacional. Busca-se fazer um questionamento se isso é suficiente para demonstrar depois da organização para tratar do assunto de forma global.

Inicialmente, serão discutidos os modelos adotados pelo Brasil, pela União Europeia e outros países em suas leis de proteção de dados, para, posteriormente, falarmos da internet fechada, como na China.

5.1 OS CAMINHOS ENCONTRADOS NAS LEGISLAÇÕES PARA PROTEGER-SE DA INTERNET GLOBAL

O início dá-se pela análise de quais dados serão objeto das legislações. Ambas as principais legislações que estão sendo analisadas nessa dissertação, a lei brasileira e a lei europeia, levam em consideração um critério definidor para qual dado está sendo objeto de proteção como um princípio de razoabilidade sobre o processamento desse dado.

Para o artigo 5º, inciso I da lei brasileira, *dado pessoal* é qualquer dado que é identificável ao indivíduo. Para um dado estar dentro do espectro da proteção da lei, não basta que o dado esteja atrelado a um indivíduo. Para definir se o dado é identificável ao indivíduo, essa vinculação tem de passar por um esforço razoável para reverter qualquer método de ocultar a identidade do sujeito do dado empregado por quem o processou.

Esse processo que tem por objetivo desvincular o sujeito e transformar o dado em informação que não está diretamente ligada ao indivíduo é o processo de anonimização. Esse perímetro de elasticidade do conceito de dado pessoal depende do processo que o fará identificável ou não. Além disso, o que se entende por razoável tem critério definido pela legislação. A determinação é que devem ser levados em conta critérios objetivos de tempo necessários para reverter esse processo de

anonimização do dado. Além do tempo, são consideradas mais as tecnologias disponíveis e a utilização de meios próprios para verificar se este dado está dentro deste critério (BIONI, 2019, p. 76).

Este ponto é necessário para definir qual dado está sendo objeto de proteção. Não se protege apenas os dados que têm relação direta com a identificação do indivíduo, mas aqueles também que podem gerar identificação dentro de um esforço razoável. É o conceito que as legislações trazem de dado pessoal.

Relevante destacar a importância de se estender a proteção ao dado identificável exposto anteriormente. A internet funciona de tal forma que não é necessário saber a identidade do usuário para sujeitá-lo a conteúdo direcionado ou decisão automatizada. Basta o atribuir um identificador, como o número de IP atribuído ao computador que ele está conectado. A partir dele, se reconhece o dispositivo e os *logins* a ele relacionados. Assim, forma-se um perfil comportamental da sua navegação. Por essa razão, a premissa regulatória de proteger o cidadão a distinção absoluta entre dados pessoais e anonimizados perde o sentido (BIONI, 2019, p. 77-78).

Outro conceito de extrema é o de dados pessoais sensíveis. O artigo 5º, inciso II, da Lei Geral de Proteção de Dados Pessoais brasileira determina que dados sensíveis são dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização religiosa, filosófica ou política. Podem ser também dados referentes à saúde, a vida sexual, dado genético ou biométrico quando vinculado à pessoa natural.

O intuito de criar essa proteção é coibir práticas discriminatórias e assegurar ao usuário tenha liberdade para se relacionar e se realizar perante a sociedade, sem que eventuais práticas discriminatórias frustrem tal projeto (BIONI, 2019, p. 86).

A característica particular desses dados sensíveis faz com que tanto a LGPD brasileira, quanto a GDPR europeia criem hipóteses mais restritivas para o tratamento de dados sensíveis. Dentre as previsões, destaca-se o consentimento especial para tanto do titular dos dados, como contrapeso do risco inerente ao tratamento de dados sensíveis (BIONI, 2019, p. 229). A legislação brasileira define essas proteções extras no artigo 11. O inciso primeiro destaca a necessidade de um consentimento específico e destacado, com finalidade específica para o tratamento de dados sensíveis. Já o inciso segundo dispõe os casos em que não se é preciso o consentimento, limitando-

os em obrigação legal ou regulatória do controlador dos dados, dados necessários a administração pública para aplicação de políticas previstas em lei ou regulamento, estudos por órgãos de pesquisa, garantida a anonimização sempre que possível, exercício regular de direitos, proteção da vida ou da integridade física do titular ou de terceiro e, por fim, prevenção a fraudes e garantia da segurança do titular nos processos de identificação e autenticação de cadastros em sistemas eletrônicos, com exceções previstas na lei.

Dito isso, passa-se a tomar uma abordagem maior do aspecto territorial das legislações de dados pessoais. A União Europeia optou por transformar sua lei de proteção de dados em uma lei de efeito direto. Isso significa dizer que os cidadãos europeus podem fazer uso dela em seus tribunais nacionais sem que exista qualquer referência em legislações internas desses países. O que faz com que seja desnecessário para um país da união legislar em repetição sobre o assunto (DIXON, 2018, p. 30).

Mais importante, o legislador europeu tentou conferir à lei um alcance extraterritorial. Para tanto, ela se aplica a qualquer organização que atue dentro da União Europeia, mesmo que sua sede não esteja localizada em um de seus países. Qualquer organização, de qualquer setor ou tamanho, que processe dados pessoais, precisa respeitar a *General Data Protection Regulation* (GDPR), seja governo, provedor de internet, veículos de mídia, bancos, consultórios médicos ou universidades. Qualquer organização que colete informações digitais sobre seus usuários (DIXON, 2018, p. 30).

Para esse sistema funcionar, a legislação europeia criou o princípio de responsabilidade ou responsabilização[1]. Este princípio é tido como a maior inovação trazida pelo legislador e a pedra fundamental do sistema. Este entrega toda a responsabilidade sobre a coleta e processamento de dados nas organizações que os fazem, assim, podendo entregar ao indivíduo o direito de evitar a atuação destas, se assim desejar (DIXON, 2018, p. 30).

Este princípio encontra-se nos artigos 26 e 27 da GDPR. O artigo 26 dispõe que quando dois ou mais organizações são responsáveis pelo tratamento de dados pessoais, ambos são responsáveis em conjunto. Estão obrigados a determinar com transparência as respectivas responsabilidades pelo cumprimento da legislação no

[1] Em tradução livre do *principle of accountability*.

que diz respeito ao exercício do direito do titular dos dados e no dever de informação, na medida de sua responsabilidade determinadas pelo direito comunitário europeu ou do Estado membro que faça parte. Esse acordo que determina a responsabilidade deve refletir as funções e relações com o titular do dado e a essência do acordo deve ser de conhecimento do titular.

Já o artigo 27 determina que este responsável deve estar sempre dentro da União Europeia, em designação por escrito, exceto as operações que não exerçam capitação de dados em grande escala, ou que não abranjam dados sensíveis, nem impliquem em risco direitos e liberdades individuais. Também encontra exceção em capitação de dados de autoridades e organismos públicos.

A lei determina também que este representante esteja sempre em um Estado membro em que se encontra o titular do dado objeto de tratamento, no contexto da atividade e da oferta que é feita de bens ou serviços. Assim, esse representante assume a responsabilidade pelo tratamento de dados ou pelo subcontratado que não estiver na União Europeia, em complemento ou em substituição relativamente a todas as questões relacionadas ao tratamento de dados. A *GDPR* também dá ao sujeito do dado o direito de requerer que este seja apagado ou de mover esses dados de uma organização para outra. Uma portabilidade de dados (DIXON, 2018, p. 30).

Para que isso ocorra de forma certa, as organizações que desejam processar dados precisam ter um funcionário responsável por garantir o cumprimento da legislação, o *data protection officer*. Também são obrigados a realizar estudos para determinar o impacto da coleta de dados no indivíduo. Portanto, seus sistemas terão de ser arquitetados de tal forma a limitar os dados que podem ser coletados, bem como garantir a segurança desses dados. Por fim, em caso de vazamentos dos dados coletados que exponha a risco os indivíduos, essas organizações estão obrigadas a notificar as autoridades. Por fim, existe uma obrigação de transparência, na qual devem prestar informações claras e detalhadas de quais e por qual razão esses dados estão sendo coletados (DIXON, 2018, p. 30).

Para tentar garantir eficácia, a lei europeia confere aos reguladores novas formas de forçar o cumprimento dessas normas, como emitir liminares e a autoridade para aplicar pesadas multas pecuniárias nas organizações que falharem em seguir com o determinado (DIXON, 2018, p. 31).

Assim, a GDPR se preocupou em criar, em seu artigo 17, parágrafo 3º, nº1, seu âmbito territorial, ao dizer que se aplica a todos os tratamentos de dados pessoais efetuados no contexto de atividades do responsável do tratamento que se manifestem em território europeu, independente desse processo ocorrer ou não na Europa. Assim, percebe-se que a GDPR quer ser global, porém, a extensão territorial dos direitos criados pela regulação não o são. Estes irão variar da pretensão do titular do direito. Ao se analisar literalmente o texto do regulamento europeu, percebe-se que podem potencialmente ser utilizado para toda a internet como ferramenta jurídica para salvaguardar a proteção de suas informações pessoais (ARGA E LIMA; CARVALHO, 2019, p. 62).

A lei brasileira, em seu artigo 3º, buscou também um alcance extraterritorial. A legislação tem como alcance qualquer operação de tratamento de dados, seja ele realizado por pessoa física ou por pessoa jurídica, de qualquer tamanho ou atuação, de direito público ou privado, independente do meio, do país de sua sede ou do país de que estejam localizados. Assim sendo, a proteção de dados se dá mesmo contra organizações de outros países.

Para que essas organizações, mesmo internacionais, sejam alcançadas pela lei brasileira de proteção de dados, elas precisam atuar em algumas hipóteses. A primeira é a de o tratamento de dados estar localizado em território nacional. A segunda é a de esse tratamento de dados ter por objetivo a oferta ou fornecimento de algum tipo de bem ou serviço para alguém localizado no Brasil. A terceira é o dado pessoal, mesmo que de estrangeiro por empresa estrangeira, tenha sido coletado dentro do território nacional. Para tanto, o primeiro parágrafo busca o esclarecimento que dado coletado em território nacional é aquele que, quando coletado, o indivíduo ao qual este se refere estar dentro das fronteiras brasileiras.

Ainda no âmbito do tratamento internacional dos dados, os artigos 33 e seguintes da lei de proteção de dados brasileira só permitem a transferência internacional de dados pessoais na hipótese de ser feita para países ou organizações que promovam a proteção de dados semelhantes às da brasileira, bem como quando o controlador de dados garantir dos princípios da lei brasileira, dos direitos do titular e do regime de proteção de dados. Quem deve averiguar o cumprimento de outro país com os mesmos princípios brasileiros é a autoridade nacional.

Existem outras situações em que a transferência é permitida pela legislação brasileira: quando a transferência for necessária para cooperação internacional; quando necessária para a proteção da vida; com autorização da autoridade nacional responsável; quando resultar de compromisso assumido em acordo internacional; quando necessário para alguma política pública; e com consentimento específico do sujeito dos dados.

A razão da lei europeia e da lei brasileira serem tratadas com proximidade é porque a nacional sofreu grande influência da europeia. Elas são semelhantes em muitos aspectos. Começam apresentando o objeto e objetivo da lei, explicando a matéria que buscam cuidar e o seu alcance territorial. Em seguida, apresentam definições para compreensão da lei. Depois, apresentam os princípios relativos à proteção de dados.

Os princípios da lei brasileira são extremamente semelhantes àqueles presentes na legislação europeia. Em continuação, ambas as leis colocam um caráter central no consentimento. Aos direitos dos usuários dos dados, como a informação de como deter acesso aos dados e de como retificá-los e cancelá-los. Ambas as legislações apresentam limitações semelhantes ao tratamento dos dados, em especial no que se refere ao atendimento de interesse público e a importância da cooperação nacional e internacional para segurança no tratamento de dados. Mais semelhanças se apresentam nos valores das infrações que podem ser impostas, sendo 2% do faturamento em seu último exercício, ou R$ 50 milhões (PEREIRA, 2019, p. 28).

Porém, há críticas que são feitas contra a lei brasileira que não são repetidas pela lei europeia. A brasileira não define um órgão independente e suas qualificações para a fiscalização e controle de dados, dificultando o entendimento de como será o procedimento de notificação de violação à autoridade de proteção de dados. Outra crítica é a forma superficial e genérica que é dado à certificação, bem como de seles e marcas de proteção de dados, voltados à comprovação da conformidade com as regras da lei (PEREIRA, 2019, p. 29).

Coloca-se essa comparação entre essas duas legislações também porque as leis de proteção de dados pessoais são um arranjo de governança. São normas que abraçam todo e qualquer processamento de dados que sujeite uma pessoa individualmente ou um grupo de pessoas ao processamento de dados. O que importa é o impacto que provoca na vida do indivíduo ou do coletivo ao qual o dado se refere.

Por essa razão, se reforça a necessidade do entendimento da proteção de dados pessoais como um direito da personalidade. Permite-se, assim, um alcance maior para a proteção. O foco está na consequência da atividade de processamento de dados sobre o sujeito. O que importa é o uso, não o dado (BIONI, 2019, p. 80). Tanto a legislação europeia, como a brasileira, atuam da mesma forma, por isso são tratadas em conjunto.

Outro exemplo é o da legislação de dados pessoais da Argentina, tida como uma das mais avançadas quando foi criada. Primeiramente, estabelece legalidade dos bancos de dados, com registro em um órgão específico do governo, protegendo o conjunto de dados pessoais coletados e processados, eletronicamente ou não, em qualquer formato, modelo de armazenamento, disposição ou acesso. A lei fala a respeito da qualidade dos dados, segurança e confidencialidade, consenso do sujeito do dado, condições específicas para a transferência interestatal dos dados, com responsabilidade solidária entre o sujeito que coletou o dado e um terceiro contratado. Fala também do direito do sujeito dos dados, como acesso à informação, retificação, atualização ou suspensão, *Habeas Data*, requisitos e procedimentos quanto ao registro do banco de dados, além de sanções penais e outras disposições (MILANÉS, 2017, p. 36).

O Chile é o primeiro país latino-americano a ter uma legislação especial para a proteção de dados pessoais, desde 1999. Porém, esse documento legal se provou ineficaz com o passar do tempo em proteger o usuário, facilitar transferência internacional de dados e se ajustar aos padrões internacionais. Portanto, desde 2011, uma nova legislação está sendo discutida no país. Apesar de diversas críticas sobre a possibilidade de prejudicar a competitividade do Chile no mercado internacional, a legislação cria uma compensação por processamento ilegal de seus dados, porém, deixa a cargo do usuário provar essa ilegalidade. Outros dois problemas apontados são a criação de barreiras para transferência de dados para dentro do Chile e da falta de possibilidade de execução mediante atores privados. Assim, cria-se uma situação em que o Chile se encontra impedido de ter seus atores atuando na União Europeia, sendo necessária uma adequação da legislação como feito na Argentina, Brasil e outros países (CERDA, 2017, p. 80).

No Uruguai, a principal lei sobre proteção de dados é de 2008, no arfam de conceder liberdades fundamentais que faltaram durante os períodos de governos não

democráticos. A lei 18.331/18, ampliada pelo decreto nº 414/19, a lei de proteção de dados pessoais e do *Habeas Data* são o centro deste direito no país. A legislação cria princípios aplicáveis a todos no contexto da coleta e processamento de dados, bem como os princípios de proteção, os direitos de acesso à informação, acesso, retificação, supressão de dados, proteção especial para dados sensíveis, disposições especiais para publicidade, para bancos de dados de consumo e telecomunicações, além de regras para transferência internacional de dados, registro de banco de dados obrigatório e, finalmente, a criação da Unidade Reguladora e de Controle de Dados Pessoais, que tem atuação igual à de uma Autoridade de Proteção de Dados (GUIDI, 2018, p. 101). Vale ressaltar que o Uruguai e a Argentina criaram essas legislações muito antes do Brasil.

Essa agilidade se dá, no caso uruguaio, por sua inspiração vir da Diretiva 95/46/CE, a antecessora da GDPR na União Europeia. Porém, aponta-se uma questão fundamental: o modelo uruguaio promove uma judicialização das questões. A autoridade uruguaia não detém poder decisório para resolver questões entre um indivíduo e um ente público ou privado. Cabe a Autoridade apenas indicar a jurisdição correta que o cidadão deve se valer para buscar seu direito. Assim, não há no Uruguai uma instância administrativa, cabendo como solução apenas o poder judiciário local, pelo instrumento do *Habeas Data.* Por este, pode pedir não só a informação, mas também a retificação, inclusão ou supressão de dados (GUIDI, 2018, p. 103).

A crítica que se faz ao modelo adotado por esses países está no peso do consentimento. As capacidades cognitivas do ser humano e sua racionalidade são limitadas. Não é crível que seja capaz de absorver, memorizar e processar todas as informações relevantes para o processo de decisões. Já é impossível memorizar todos os atores que mineram os dados de usuários, então, também é impossível compreender como os dados pessoais serão tratados por esses atores, já que cada um tem suas respectivas políticas de privacidade. Inclusive, existe ainda o complicador de se compreender como a agregação dos dados pessoais conseguem extrair informações detalhadas sobre o usuário (BIONI, 2019, p. 147).

As legislações tratam da vulnerabilidade do usuário. Porém, apostam suas fichas em que a parte mais fraca da relação é quem é o sujeito racional, livre e capaz para fazer valer a proteção dos seus dados pessoais. Assim, o protagonismo do consentimento cai em uma contradição intrínseca. O consentimento é visto como o

pilar da estratégica regulatória adotada, porém, mais como um meio de legitimar os modelos de negócio da economia digital do que como um meio de promoção da proteção dos dados pessoais. É considerado uma mistificação, na medida em que não é confrontado com a vulnerabilidade do usuário, que dificulta a liberdade e a autodeterminação dele sobre seus dados pessoais (BIONI, 2019, p. 167).

Uma perspectiva diferente é a proteção de dados nos Estados Unidos, país onde estão localizados os principais atores da internet global. O país não tem legislação federal sobre proteção de dados pessoais. Porém, sua legislação trata do assunto de forma setorial. Existem legislações especiais para crianças e adolescentes, dados médicos ou de saúde, dados financeiros e de dados de pessoas inseridas no contexto de comunicação eletrônica. Porém, não há uma legislação federal que tenha por objetivo criar um direito unificado de proteção de dados, suas regras e princípios.

Destacam-se algumas leis federais com âmbito setorial. Primeiro o *Electronic Communication Privacy Act*, de 1986, que é formado pelo *Wiretap Act*, pelo *Stored Communication Act* e *Pen Register Act*. Enquanto o *Wiretap Act* protege os cidadãos contra atos tanto de entes privados como públicos de interceptação, uso ou revelação das comunicações telefônicas, orais ou eletrônicas, o *Store Communication Act* diz respeito a dados armazenados de comunicação e de cadastro armazenados pelos provedores de serviço. Por fim, o *Pen Register Act* versa sobre o uso de dispositivos para rastreamento de chamadas.

Outra lei setorial importante de proteção de dados de escopo federal é o *Children's Online Privacy Protection Act* (COPPA), de 1998. Essa legislação cria proteção especial à privacidade para menores de 13 anos online. A lei especial para dados proteção e privacidade de dados médicos é o *Health Insurance Portability and Accountability Act* (HIPAA), de 1996. Essa legislação fala, entre outras coisas, sobre padrões de segurança, condições básicas para tratamento justo e legal de dados pessoais e situações em que o consentimento é dispensado, direito de acesso aos dados e informações sobre tratamentos. Por fim, destaca-se o *Privacy Act,* de 1974. Essa é a legislação que estabelece os princípios e as regras para a coleta, armazenamento, uso e comunicação de dados pessoais em atividades conduzidas por agências federais (GUIDI, 2019, p. 424).

Por esse sistema sem uma legislação específica não há entidade responsável pela observância do cumprimento da proteção de dados. No lugar dessa autoridade, várias entidades, públicas ou privadas, operam a fiscalização do tratamento de dados. São essas entidades, agindo como agências reguladoras, que irão impor o cumprimento dessas legislações. Assim, cada agência responsável pela fiscalização do setor de aplicação daquela legislação o faz também sobre a proteção de dados em sua área de abrangência. Os exemplos são o *Federal Trade Commission* ser responsável pela fiscalização e aplicação do COPPA e das regras referentes ao direito do consumidor, como abuso na coleta e utilização de dados de consumidores, segundo seu estatuto, ou o *Department of Health and Human Services*, responsável pela aplicação do HIPAA e do *Consumer Financial Protection Bureau* para o setor financeiro (GUIDI, 2019, p. 425).

Assim, por mais que a legislação americana entenda a proteção de dados como relacionada com o direito da privacidade e com o controle que exerce sobre a vida particular, sua extensão é incerta e desigual em suas limitações. Existe um direito a avaliação do peso de sua privacidade na avaliação pelos tribunais de seu caso concreto, mas o real alcance da proteção será definido pelo judiciário. Assim, esse direito dificilmente é autoaplicável ou diretamente exigível pelo titular dos dados.

Desta forma, para os Estados Unidos, a proteção de dados ainda não alcança um estatuto de direito fundamental ou de direito humano. A constituição americana está mais voltada para proteger a liberdade e garantir não ingerência do Estado, tendo pouca aplicação em relações privadas. Dessa forma, o contrato é alavancado como a norma mais próxima ao indivíduo. Assim, fica a cargo das partes, dos usuários e dos entes que manipulam os dados definir o que será tido como justo e razoável, tendo-se a liberdade contratual como força máxima nessa relação.

O modelo americano tem como principal pilar o consentimento, porém, de forma diferente do que observado no modelo europeu. Em exceção de situações específicas, no modelo norte-americano, para que sejam coletados dados de um indivíduo, não se requer que haja correlação com sua atividade. Quem coleta não precisa justificar finalidade, mas dar transparência sobre o que está sendo coletado. As liberdades para tomar decisões são fundadas pelas informações adequadas. Assim, surgem as políticas de privacidade das empresas e o consentimento é a

consequência presente nas políticas de privacidade e das estratégias regulatórias (GUIDI, 2019, p. 426).

Portanto, o consentimento do sistema americano não se trata de um consentimento informado, livre ou expresso. É um consentimento minimamente válido de acordo com as regras contratuais, sem que se exija uma comprovação do que foi consentido. Está mais próximo de uma venda de informações do que uma relação entre o usuário e o tratamento responsável. Essa abordagem privilegia a livre iniciativa e a inovação e permite que novidades dos usos dos dados venham a ser implementadas sem regulação. Porém, é uma abordagem que deixa o usuário vulnerável no que diz respeito da proteção de seus dados (GUIDI, 2019, p. 427).

A Califórnia apresenta uma mudança significativa. Entrou em vigor no Estado a legislação mais agressiva sobre o assunto, que se compara com à legislação europeia, objetivando melhorar como as empresas irão cuidar dos dados de seus consumidores.

A *California Consumer Privacy Act* (CCPA), que entrou em vigor em janeiro de 2020, estabeleceu o direito dos indivíduos de pedirem para as empresas informações sobre quais seus dados coletados, e de requerer que as empresas apaguem qualquer dado coletado sobre os consumidores. O ponto central da CCPA é a venda dos dados dos consumidores. A legislação obriga entrega do direito aos consumidores exigirem transparência sobre quais dados estão sendo coletados para venda e para fins comerciais, incluindo o direito de pedir a exclusão de seus dados da venda (JURCYS et al., 2020, p. 3).

Assim, os Estados Unidos são tratados de forma diferente da Europa e do Brasil. O modelo de proteção de dados brasileiro segue o europeu, enquanto o dos Estados Unidos é um modelo em que não prevê uma proteção de dados, exceto por leis especiais para situações especiais. Não há um direito de proteção assegurado como fundamental nos Estados Unidos, apesar de haver proteções específicas. Outro ponto importante é que se já é criticável o consentimento especial e qualificado do modelo europeu, o consentimento contratual do modelo americano é muito mais frágil. Esse modelo deixa ao usuário vulnerável, mesmo que permita o avanço tecnológico.

5.2 O CAMINHO DA CHINA, CRIAR FRONTEIRAS VIRTUAIS

Como dito anteriormente, algumas jurisdições podem preferir uma versão da internet em que o Estado possa exercer maior controle sobre sua população. Mais que isso, a extrema captação de dados pessoais nas mãos de um governo que deseja controlar a população, limitar suas liberdades, pode ser muito importante.

Vale, inicialmente, dizer que já há mais pessoas na China com acesso à internet do que em qualquer outro país. A China pretende criar um sistema de defesa digital intransponível, ganhar maior voz na governança da internet e fomentar suas empresas para liderar o avanço global em tecnologias. O país também criou uma agência chamada Administração do Ciberespaço da China[2], que tem por objetivo controlar conteúdo online, reforçar a segurança cibernética e desenvolver economia digital (SEGAL, 2018, p. 10).

Para tanto, a China seguiu alguns passos. Primeiro, o chamado de *internet harmoniosa*. Ou seja, guiando a opinião pública, apoia boa governança e promove crescimento econômico. Isso significa dizer que é uma internet controlada, para impedir mobilizações políticas e impedir a circulação de informações que poderiam prejudicar o governo. O segundo passo é o controle tecnológico atingido sobre inteligência artificial computação quântica e robótica. Em terceiro passo, tem-se dado maior preocupação para a cibersegurança. O Exército de Libertação do Povo anunciou planos para acelerar a criação de forças cibernéticas e para fortalecer as defesas de rede chinesas (SEGAL, 2018, p. 11).

O ponto mais importante do plano chinês é sua promoção de uma cibersoberania como princípio organizador da governança da internet. É o caminho contrário ao da internet aberta e global, como foi iniciada nos Estados Unidos. A soberania na cibernética representaria o direito de países individualmente escolherem seus próprios caminhos para o desenvolvimento cibernético, para seu modelo de regulação e políticas públicas para a internet, além de participar da governança do ciberespaço internacional em pé de igualdade.

Com isso, a China tenta criar um mundo repleto de *internets* nacionais, onde os Estados nacionais exercem controle do ambiente digital pelo direito de soberania nacional. Assim, a China pretende enfrentar o modelo definido e defendido pelos Estados Unidos e seus aliados, que é movido primeiramente pelo setor privado.

[2] Tradução livre de *Cyberspace Administration of China*.

Para os chineses, a governança da internet é dominada por empresas de tecnologia ocidentais e organizações da sociedade civil. Os chineses acreditam que teriam uma palavra maior na regulamentação da tecnologia da informação e na definição de regras globais para o ciberespaço se a Organização das Nações Unidas tivesse maior relevância na governança da Internet (SEGAL, 2018, p. 12).

Desta forma, temos um Estado visando o controle populacional e do conteúdo na internet, preferindo uma arquitetura da internet repleta de fronteiras virtuais, o contrário da rede global que existe hoje em dia.

O esforço chinês teve como consequência a construção da chamada *Great Firewall*, uma alusão à grande muralha da China, mas que se trata de um sistema que garante que o conteúdo online disponível no país seja plenamente controlado pelo governo central (SILVA, 2019, p. 36).

Mais importante para a questão dos dados pessoais é que, além de instituir censura e vigilância, os chineses criaram uma estrutura legal para melhorar a cibersegurança e a salvaguarda de dados em servidores estatais ou privados (SEGAL, 2018, p. 12). Empresas chinesas importantes, como *Baidu*, *Tencent* e *Weibo*, já foram multadas por não cumprimento a essas regras. As empresas do restante do mundo se preocupam que uma interpretação extensiva dessas regras de inspeção de equipamentos e de armazenamento de dados na própria China irá permitir que o governo roube esses dados e propriedades intelectuais (SEGAL, 2018, p. 13).

O plano Chinês busca um autoritarismo digital, uma resposta que uniria de controle social e ganhos econômicos, que são de suma importância para manter a máquina estatal apta ao monitoramento da população. Isso também serve como forma de dissuasão de revoltas populares, já que esses ganhos econômicos são aproveitados por todos, não apenas por uma pequena camada política. Compra-se, assim, a alma da população com bens e serviços (SILVA, 2019, p. 40).

Deste modo, tem-se na China uma internet fechada, controlada pelo governo, em que o Estado tem acesso aos dados. A vigilância aqui não é feita por empresas que pretendem vender publicidade, mas pelo governo, que pretende controlar comportamento. A internet global pode não ser perfeita, mas a solução adequada não parece passar pela criação de fronteiras digitais como o *Great Firewall* chinês.

Mais impactante é o uso chinês da coleta e processamento de dados no sistema de crédito social adotado pelo regime. No país, ser pego atravessando a rua fora da faixa de pedestres ou ouvindo música mais alto que o permitido irá render ao cidadão mais do que apenas uma multa. Alguns de seus direitos serão cerceados, como o de comprar passagem aérea ou de trem (KOBIE, 2019).

O sistema foi inaugurado em 2014, mas não se trata de um grande sistema de crédito para toda a China. Os governos locais mantêm sua própria pontuação. O sistema se utiliza de dados, como hábitos de consumo, para criar uma informação semelhante à pontuação. Esses pontos estão sendo usados inclusive no judiciário do país. É uma grande coleção de dados que são processados sem transparência de algoritmo sobre como são analisados para resultar na pontuação (KOBIE, 2019).

Todos os cidadãos, em todo o país, deverão ter um número de identificação ligado ao registro permanente. Algumas reportagens sobre o assunto afirmam existir, inclusive, uma *blacklist* para quem, por exemplo, deve algum valor ao Estado.

É diferente estar nessa lista e apenas ter um crédito baixo, pois pode-se chegar a perder certos direitos. Os critérios variam de acordo com a região, podendo ser desde não pagar multas, se portar de forma inadequada em trens, ultrapassar um sinal vermelho. Em algumas cidades, existe até o já referido reconhecimento facial em câmeras de vigilância sendo utilizado para detectar que atravessa a rua fora da faixa de pedestres. Alguns desses sistemas, inclusive, capturam uma quantidade tão grande de dados que pode avaliar até quanto tempo determinado cidadão joga videogames ou se tem filhos, sendo que os jogos dão uma pontuação ruim, e filhos, uma positiva. Um dos sistemas de crédito chega ao ponto de ter parceria com um site de relacionamentos, em que uma pessoa pode avaliar os pretendentes pela aparência e pelo seu crédito social (KOBIE, 2019).

O sistema avança para coletar informação de reconhecimento facial, escaneamento corporal e *geo-tracking* (rastreamento de geolocalização). É um sistema sofisticado com mais de 200 milhões câmeras de vigilância. Os dados coletados são combinados de bancos de dados governamentais, incluindo informações sobre educação e saúde, além de informações de entes privados de histórico de internet e financeiros. A pontuação pode variar em tempo real, a depender do comportamento do cidadão. Além do mais, sua pontuação é baixa não só se você cometer uma infração. Se pessoas próximas do convívio de determinado cidadão,

como um amigo ou um parente, falar algo negativo sobre o regime, este cidadão também perderá pontos (PALIN, 2018).

Os benefícios para quem está bem ranqueado podem ser hospedar-se em hotéis ou alugar carros sem depósito, tratamento especial em aeroportos, empréstimos com taxas mais baratas, prioridade em oportunidades de empregos e melhor acesso às universidades de melhor prestígio (PALIN, 2018).

Para os cidadãos que são colocados na lista, os direitos começam a ser restritos. Caso o cidadão apareça na lista de Pessoas Desonestas para Execução pela Suprema Corte Popular[3], ele não está qualificado a adquirir passagens aéreas, viajar em alguns trens, comprar propriedade ou pegar um empréstimo, sem qualquer processo, mandado policial ou notificação. Não há nada que o cidadão possa fazer a respeito. É possível buscar uma solução no judiciário chinês, porém, não há nenhuma proteção genuína dos direitos das pessoas. Assim, há um enorme potencial para o abuso de poderes. Um Estado de vigilância nacional (KOBIE, 2019).

Existem mais nações que desejam maior controle populacional. Desde 2016, a Rússia tem uma legislação que determina que as redes sociais armazenem dados sobre usuários russos em servidores dentro de seu território. Agora, os russos desejam cortar suas relações virtuais com o mundo. Para tanto, pretendem criar uma internet doméstica, completamente russa. O governo russo pode ter o poder de bloquear conteúdos e manter o tráfego entre usuários restritos ao território nacional, sem contato com entidades internacionais (SHERWIN, 2019).

Outra forma de se utilizar os dados pessoais com possibilidade de se reverter em um autoritarismo digital ocorre na Venezuela. Para um cidadão venezuelano ser capaz de comprar produtos em um mercado, ele é obrigado a fornecer nome completo, identificação, telefone, endereço, data de nascimento, além de reconhecimento biométrico em um aparelho digital (DÍAZ, 2017, p. 30).

As lojas da Venezuela são obrigadas a armazenar esses dados, por imposição dos órgãos fiscais do governo. Assim, a quantidade de dados que o governo venezuelano tem sobre seus cidadãos seria um paraíso para qualquer analista de *Big Data*. Além disso, ninguém além dos governantes sabe como esses dados são usados

[3] Em tradução livre do original em inglês no texto referenciado *Dishonest Persons Subject to Enforcement by the Supreme People's Court*.

e onde são armazenados. Quanto mais dados o governo adquire sobre seus cidadãos, mais fácil de manter um sistema de vigilância sobre eles (DÍAZ, 2017, p. 31).

A situação grava-se por se tratar da Venezuela, com um triste histórico recente de perseguição política por conta da lista de Tascón, quando foram tornadas públicas informações políticas de cidadãos. Após essa lista, muitos cidadãos se viram impedidos de acesso a crédito, educação ou oportunidades de emprego por apoiar um referendo contra o governo (DÍAZ, 2017, p. 32).

Não há regulações sobre dados pessoais na Venezuela. Assim, o governo venezuelano detém uma grande quantidade de dados pessoais sem que seu destino seja de conhecimento da população. E mais, o órgão estatal responsável por fiscalizar a atividade bancária ordenou aos bancos que entreguem ao governo todas as informações sobre transações digitais no país, incluindo endereço de IP, quantias, nomes, contas bancárias e o motivo da transação (DÍAZ, 2017, p. 32).

Trata-se de um sistema vulnerável. Mesmo para quem não teme o governo, a segurança desse sistema é dúbia. Informações sobre registro civil e eleitoral, bem como informações fiscais e de seguridade social são públicas. Podem ser consultadas online e mineradas livremente. Não é um sistema ao qual se deseja confiar suas informações pessoais, mas, caso o cidadão não deseje fornecer seus dados, ele será impedido de comprar produtos de necessidade básica (DÍAZ, 2017, p. 33).

A internet global, como vista anteriormente, é uma evolução importante demais para ser desprezada pelas nações em defesa de interesses de controle de comportamento. Como visto anteriormente, é uma ferramenta de proteção de direitos humanos, porém, que tem problemas que devem ser resolvidos sem extinguir sua melhor característica, sua capacidade de integrar o mundo em uma grande rede.

6 A HIPÓTESE DE UMA ORGANIZAÇÃO INTERNACIONAL VISANDO A PROMOÇÃO DA PROTEÇÃO DE DADOS PESSOAIS

Este capítulo tem por objetivo demonstrar a hipótese apresentada de uma organização internacional com o intuito de promover uma proteção uniforme, eficaz e global da organização internacional, cuidando de possíveis conflitos de jurisdição. Visa promover também uma proteção de cooperação entre as nações quanto ao tema, dando cobertura a todos os usuários da rede.

Primeiramente, destaca-se a crescente contribuição das organizações internacionais para o direito internacional, na qual, em grande parte dos casos, seus efeitos não são devidamente creditados. A atuação das organizações internacionais é um elemento de significativa relevância na formulação de costumes internacionais e na importância das notas de direito internacionais que operam por essas organizações (SHAW, 2011, p. 1.295).

Destaca-se também que o papel que uma organização internacional opera no mundo é centrado em torno da posse de personalidade jurídica internacional. Essas instituições são capazes de exercer direitos e deveres no plano internacional, independente da personalidade doméstica dentro do Estado em que se encontra. Elas advêm, principalmente, de seus poderes, propósitos e de sua atuação (SHAW, 2011, p. 1.297). Desta forma, uma personalidade jurídica própria é importante para a capacidade de atuação da organização internacional de forma direta, para permitir sua ação sem a dependência de algum de seus Estados membros (SHAW, 2011, p. 1.299).

No entanto, a personalidade jurídica internacional não pode ser confundida com a personalidade doméstica que a instituição pode deter para ser proprietário do seu imóvel sede. A personalidade jurídica doméstica dependerá do Estado em que a organização estiver sediada (SHAW, 2011, p. 1.299). A personalidade jurídica internacional irá variar de acordo com as circunstâncias.

Organizações dotadas de personalidade jurídica terão direitos e deveres, porém, não terão a mesma capacidade. Também, irá variar a forma como serão exercidos os direitos e deveres. Enquanto os Estados detêm em totalidade a personalidade jurídica, para as organizações, ela será limitada pelo instrumento constituinte ou pela prática recorrente necessário para a realização de suas atividades (SHAW, 2011, p. 1.302).

Concluindo o debate sobre a personalidade jurídica, parece que é de vital importância para a organização que seja interesse a promoção de dados pessoais para que tal personalidade seja lida como jurídica. Para atingir todos os seus objetivos, como veremos mais adiante, é imprescindível que ela seja capaz de agir por conta própria no cenário internacional. Isso impõe deveres e direitos para a atuação total da organização perante os Estados e demais atores do ambiente digital.

Francisco Rezek (2010, p. 275) apresenta uma distinção entre as espécies de organizações internacionais. Para tanto, leva em conta o alcance da organização, seja ela universal ou regional. As organizações universais são aquelas que podem receber como seus membros a maior quantidade possível de Estados, sem qualquer restrição geográfica, cultural, econômica ou outras. Também há distinções quanto ao domínio da atividade da organização, divididas em duas categorias, as de vocação política - que visam a manutenção da paz - ou as de vocação específica - voltadas primordialmente a um fim econômico, financeiro, cultural ou estritamente técnico.

A organização pensada nesta dissertação tem seu alcance global, uma vista que tem por objetivo atender a todos, por pensar na proteção de dados pessoais como um direito universal. Assim, é de vital importância para a eficácia da organização em atingir seu objetivo que ela alcance o maior número possível de Estados. Também a organização tem uma vocação específica voltada à promoção do direito de proteção de dados pessoais.

Passando a falar da organização interna da organização, dois órgãos aparecem como indispensáveis para sua estrutura: uma assembleia geral, na qual todos os membros detêm a mesma voz e o mesmo direito a voto, e na qual serão tomadas as decisões que irão criar as regras; e as legislações da entidade, bem como uma secretaria, um órgão administrativo com funcionários permanentes (REZEK, 2010, p. 259).

Para a organização hipotética deste trabalho, a assembleia geral será a responsável por desenvolver os princípios bem como a legislação de promoção de dados pessoais, que deverão ser comuns a todos os Estados membros. Para tanto, não apenas os Estados, como as empresas, também devem se manifestar, bem como algum representante da sociedade civil. Assim, esses entes privados e da sociedade civil poderão contar com o direito a pelo menos um voto e participarão no estabelecimento dos regramentos da organização.

Rezek (2010, p. 261) tece alguns comentários sobre o processo decisório utilizado pelas organizações internacionais. De um modo geral, as organizações ainda não evoluíram até um ponto em que o voto por maioria se aplique de forma semelhante ao direito interno. Um Estado só costuma se sentir obrigado quando se tenha decidido com seu voto favorável, quando atua em assembleia ou conselho de uma organização internacional, naquilo que se considera mais importante, e não

apenas instrumental, como a eleição de algum cargo interno da organização ou a fixação de calendários de trabalho.

Trazendo as empresas e a sociedade civil para o processo decisório da organização internacional, visa-se uma solução nos moldes da governança global. Governança refere-se a diferentes formas de regulações que não são a atividade tradicional de um Estado, hierarquizado. A governança implica na autorregulamentação de atores da sociedade, buscando soluções de problemas da própria sociedade. Também a governança se refere a novas formas de políticas e vários níveis.

Porém, uma ideia de governança global ainda pende pelo meio acadêmico de uma definição clara. Nos anos de 1990, se debatia a governança global como um novo parâmetro para o multilateralismo e cooperação interestatal. Depois dos anos 2000, o enfoque modificou para os desenvolvimentos de transformação das políticas globais (BIERMANN e PATTBERG, 2012, p. 3).

São dois os usos mais amplos para governança global. Primeiro, o conceito usado em um sentido analítico, como a descrição de transformações atuais das sociopolíticas. Neste sentido, a noção de governança global destaca as distintas características das políticas mundiais, como modos de direção não hierárquica e a inclusão de atores privados, ambos com ou sem fins lucrativos. O segundo conceito é usado como a descrição do programa político que lida com os desafios da globalização. Assim, a governança global começa com a notória inadequação de respostas ao mundo globalizado. Portanto, governança global conceitua-se como um programa político para ganhar novamente a necessária capacidade de direção para resolver problemas da idade pós-moderna (BIERMANN E PATTBERG, 2012, p. 4).

Neste espectro, os três aspectos fundamentais da governança são primeiro, como um meio e processo capazes de produzir resultados eficazes. A participação ampliada, por incluir não só os Estados, mas também a empresas e a representantes da sociedade. Por fim, a busca por um consenso (GONÇALVES E FONTOURA, 2011, p. 53).

Assim, em se tratando de uma organização internacional que visa a participação não hierárquica de Estados e empresas, bem como de representantes da sociedade civil, para a solução de um problema global, que as sociedades

modernas têm dificuldade em solucionar, a organização se apresenta como uma solução de governança global.

É visto que organizações multilaterais são exemplos de sistema de governança sem uma autoridade centralizada. Cada uma foi criada para tratar de temas transnacionais específicos. Os países participantes, ao compartilhar valores, interesses e objetivos, são os pilares de funcionamento destas entidades e isso dá a eles a qualificação de sistema de governança. Os temas são debatidos por negociadores representando os países participantes, objetivando acordos para definir normas de comportamento a serem seguidos por todos.

A legitimidade dessas normas se dá pelo reconhecimento dos países participantes, estando elas de acordo com seus objetivos e interesses e se comprometem a cumpri-las inteiramente. O cumprimento se dá com a internalização de legislações nos países membros. Um país que não esteja alinhado aos valores e diretrizes não fará parte do sistema de governança. Se um pequeno número de países compartilhar desses valores, então, esse sistema não funcionará, uma vez que não ordenará determinado comportamento (VOIVODIC, 2010, p.59). Este é o desafio a ser enfrentado pela organização proposta como um instrumento de governança global: fazer com que a comunidade internacional se interesse pelo tema a ponto de criar um arcabouço legal uniforme em todo o mundo, com a adesão dos mais relevantes países do mundo, se não sua totalidade.

O presente trabalho não é a primeira hipótese de uma organização internacional a ser enxergada para a solução dos problemas da internet global. Já foi apresentada anteriormente a proposta de um Tribunal Internacional para a Internet.

Em razão da dificuldade que as jurisdições têm para enfrentar a internet dentro dos Poderes Judiciais nacionais, a necessidade de novas saídas judicantes internacionais, adequadas ao tempo da internet se faz presente. Frente aos novos problemas internacionais presentes na internet, novas alternativas cosmopolitas se apresentam como solução. Por isso foi idealizada e se considera a implementação de tal Tribunal Internacional para o Direito da Internet.

Busca-se responder aos principais desafios alinhavados do exercício da prestação jurisdicional de questões que surgem no ambiente digital. A internet tem alcançado um espaço que está intimamente ligado a diversas e importantes tarefas das pessoas e das empresas, a elevação de critérios normativos, com a consagração

de meios judiciais para possibilitar o exercício do Direito na internet é exigência primordial da sociedade atual (FREIRE E ALMEIDA, 2015, p. 380).

Seguindo essa linha de raciocínio, promove-se a presente dissertação, em que formula a hipótese de uma organização internacional com o objetivo claro de tratar da proteção de dados pelo mundo. A internet e o modelo econômico criado por ela promovem a transferência, processamento e manipulação de dados em escala global.

Existem ainda muitas lacunas nesse direito de proteção, muitas ainda desprotegidas. Este trabalho já apresentou muitos desafios a serem ainda superados pelas legislações nacionais que entram em vigor a esse respeito. Portanto, apresenta-se uma organização internacional como o instrumento de governança desses dados pessoais na internet.

6.1 OS ESTADOS E AS JURISDIÇÕES DENTRO DA ORGANIZAÇÃO

As organizações internacionais são criadas por Estados. Estes estabelecem a natureza, seu *status* e sua autoridade. Assim, estabelecem seus instrumentos constitutivos com dupla natureza. Não são apenas tratados multilaterais, vinculando os Estados membros, entrando assim como lei internacional de tratados, bem como têm caráter especial por serem instrumentos para a criação de sujeitos de direito internacional (SHAW, 2011, p. 1303). Mais que isso, os instrumentos constitutivos são organismos vivos que estão em constante desenvolvimento para manter o propósito da organização em diferentes circunstâncias (SHAW, 2011, p. 1306).

Assim, o instrumento de constitutivo dessa organização deverá preconizar desde já os princípios e regulamentos de proteção de dados pessoais a serem observados por todos os Estados membros. Ele irá definir qual a legislação a ser adotada para a proteção de dados, vinculando todos os Estados que fizerem parte da sociedade a uma proteção adequada. Este é o dever imposto de seguir as normas da organização a todo o Estado membro que fizer parte e internalizar sua legislação na legislação pátria.

Os Estados membros devem decidir sobre a sede em que a organização estará localizada: se ela estará em um país europeu, onde os esforços para a criação de uma legislação eficaz para a proteção de dados pessoais é antiga e se impulsionou a formatação dessas legislações com a GDPR; se nos Estados Unidos, no estado da

Califórnia, para se aproximar das empresas dominantes do Vale do Silício, que, como será abordado, precisam fazer parte da sociedade; ou, se essa organização deva ser sediada em algum outro local que não apresente tanta influência sobre as decisões que serão tomadas, parece que o local mais adequado para a sede dessa organização é na Europa, talvez em Genebra, para se aproximar de outras organizações internacionais relevantes. Porém, seus braços devem ser espalhados por todo o mundo. Deve ter escritórios espalhados pelo globo, para que tenha proximidade dos mais distantes usuários da internet.

Para viabilizar esse tipo de amplitude de atuação, é preciso refletir sobre o financiamento da organização. A princípio, uma contribuição deve ser requerida aos estados membros, mas uma contribuição deve vir também das organizações da sociedade civil que fazem parte da estrutura de participação ampliada da organização. Sem falar em multas financeiras para os Estados que desrespeitarem as regras da organização internacional. Por fim, o financiamento da organização deve receber apoio com um sistema de venda de selo de confirmação de conformidade e transparência, como será mais aprodundado ao se discutir o papel das empresas privadas dentro da organização.

6.1.1 A tentativa de uniformizar o direito de proteção de dados pessoais no mundo

Um dos objetivos da organização é tentar fazer uniforme a proteção de dados pessoais no mundo. Para tanto, será preciso promover a admissão do maior número possível de Estados para seu rol.

Como dito por Patrícia Peck (2018, p. 127), quando se trata de inovação tecnológica pensando em um mundo conectado e globalizado, é de extrema importância a capacidade de criar legislações mais uniformes e internacionais para que se atinja segurança jurídica para os indivíduos e instituições. Assim, em existindo um estatuto legal único, padronizado, determinando direitos, obrigações responsabilidades, quando ocorrer determinado fato, o direito estará preparado.

A admissão de novos Estados membros estará disciplinada no ato constitutivo da organização. Nele, devem ser abordadas primeiramente as condições de ingresso estabelecidas no ato constitutivo, a adesão expressa à carta e, por fim, a aceitação da adesão pelos outros Estados membros (REZEK, 2010, p. 270). Ao aderir à carta, o Estado aderirá a toda legislação de proteção de dados já constituída pela organização, ampliando assim a rede de proteção, atendendo o maior número de indivíduos.

Entende-se que o modelo legal mais adequado para a proteção de dados pessoais é aquele que está inserido dentro da legislação europeia sobre o assunto. Porém, isso é algo que precisa passar por aprovação da assembleia da organização depois desta ser formada. Algumas das normas só podem ser criadas depois da existência da organização, que deverá se adequar a realidade presente para o momento em que ela for formada.

Porém, quando um Estado membro não cumpre com as obrigações assumidas perante a organização, as consequências são as sanções previstas pelo tratado constitutivo e aplicadas pela própria organização, podendo ser desde a suspensão de determinados direitos, até a exclusão do Estado do quadro de membros (REZEK, 2010, p. 272).

Para a organização hipotética, a perda de um Estado membro representa o oposto do objetivo que se planeja, que é o de uma proteção global. Portanto, antes de se falar na exclusão de um membro, é preciso pensar em outros mecanismos como multas e sanções diferentes, como a perda do direito a voto, ou a limitação dos direitos para a cooperação estatal dentro da entidade.

Essas multas e sanções diferentes precisam, necessariamente, ser pensadas com cobrança de valores monetários. As multas podem ajudar a organização a se manter economicamente viável. Assim, além da possibilidade de perda do direito a voto ou limitação de cooperação, uma multa pecuniária será requerida de um Estado Membro que não esteja atuando em conformidade com as regras definidas pela organização.

A retirada de um Estado membro pode se dar de forma voluntária. O primeiro requisito é um pré-aviso. O lapso temporal entre a manifestação de vontade de se desligar de uma organização e o efetivo rompimento do vínculo. O segundo requisito é a atualização das contas, ou seja, que o Estado se afasta com suas obrigações

financeiras com a organização estejam cumpridas (REZEK, 2010, p. 274 e 275). Por se tratar de uma horizontalização dos atores em escala internacional, é impossível impedir que se um Estado venha a denunciar o tratado e desejar sair da organização ele não o faça. Porém, só alcançará seu objetivo se a organização possuir o maior número possível de membros.

Assim, o intuito primeiro da organização é a criação de um regime internacional para a proteção de dados pessoais. Ele pretende criar uma legislação a ser incorporada nos Estados Nacionais. A conformidade com essa legislação a ser criada pela organização é preceito básico para o ingresso de um estado nessa organização. Mais que isso, a organização deverá ter uma estrutura necessária não só para realizar a fiscalização das regras, mas para criar um corpo legislativo sempre a ser atualizado com as novas tecnologias que surgirem que interfira com dados pessoais.

6.1.2 A cooperação entre jurisdições e a transferência internacional de dados

Pelo ato constitutivo, há também de se criar uma obrigação de os Estados membros fazerem parte de uma rede de cooperação que será operada pela própria entidade com o objetivo de resolver disputas de jurisdição sobre determinado tema, bem como agilizar a troca de cooperação entre jurisdições.

Pela organização, os dados e informações que uma jurisdição deve prestar a outra, bem como a possibilidade de comunicar decisões judiciais a outras jurisdições por intermédio da organização.

Assim, ao ser internalizado o novo mecanismo pelos Estados em sua legislação, não será mais necessário o meio tradicional, demorados e ineficazes, para a cooperação entre as jurisdições quando se tratar de proteção de dados pessoais, podendo o órgão responsável da organização decidir sobre a validade de se utilizar o mecanismo próprio ou o dever de se buscar a solução pelos meios tradicionais. Não se trata, contudo, de um órgão judicial. Apenas um órgão de avaliação técnica se o pedido de uma justiça estatal a outra encontra respaldo dentro dos critérios estabelecidos pela entidade.

Um aspecto importante que a organização precisa trabalhar é com a transferência internacional de dados. A GDPR define suas instruções para poder viabilizar a transferência no capítulo V. Já no primeiro artigo, o 44, se define que

qualquer transferência deve ser feita para países que detenham o mesmo nível de proteção de dados, incluindo transferência de dados de cidadãos europeus do país não pertencente à União ou da organização internacional para outro país não pertencente ou outra organização internacional. A intenção de manter a proteção seja lá para onde o dado for transferido para fora da união é o interesse que a organização proposta neste trabalho tem em criar um regime internacional para a matéria.

O papel da organização em intermediar a transferência de dados pessoais é em manter a conformidade do sistema. A primeira hipótese prevista na legislação europeia é uma transferência com base numa decisão de adequação. A União Europeia criou uma comissão especializada para isso na GDPR. Com ou sem a comissão europeia, a organização internacional pode exercer esse papel. Pode somar-se à comissão da estrutura europeia ou atuar em substituição. Para os demais lugares em que as legislações não preveem esse tipo de estrutura, a organização atuaria sozinha. Afinal, a organização tem escala global.

Os elementos que a comissão deve avaliar têm que ser os mesmos constantes no artigo 45 da GDPR. Avalia-se se o Estado destinatário respeita os direitos humanos e liberdades fundamentais, se tem legislação atualmente em vigor, o que já é missão da organização que as nações internalizem no direito próprio legislações sobre o tema, além do que é falado no artigo sobre matéria de segurança pública, defesa, segurança nacional e direito penal, bem como o respeito ao acesso de autoridades públicas aos dados pessoais. Esse artigo requer que exista um sistema de direito e de respeito aos direitos humanos, ao Estado Democrático de Direito, bem como aos demais direitos específicos quanto à matéria de proteção de dados pessoais. A legislação pede que exista um direito robusto de proteção de dados.

O mesmo critério deve ser observado pela organização. Em especial quando existe o já referido dever de internalizar essa estrutura legal. Isso entra em especial consenso com o item 2 alínea b da norma europeia, que espera o funcionamento de autoridades de controles sujeitas a organizações internacionais e o respeito aos compromissos internacionais previsto na alínea c.

Assim, o item 3 do artigo prevê que, em ata, a comissão europeia define quais países e organizações internacionais mantêm a proteção de dados em níveis satisfatórios para a União Europeia, onde também se prevê avaliação periódica de quatro em quatro anos. Essa avaliação periódica, bem como a criação de uma lista

de países e organizações internacionais que tratam com respeito à proteção de dados pessoais para fins de avaliação da manutenção do respeito faz parte crucial da atuação da organização.

A graduação dos atores globais em nível de proteção aos dados pessoais é função que a organização precisa ter pela atuação de fiscal desse direito no mundo. A revisão periódica é também de grande importância, uma vez que o ranqueamento não pode ser fixo. Uma nação pode criar ou revogar direitos que podem modificar seu patamar e confiabilidade para a transferência internacional de dados. Isso acarreta, inclusive, não só na queda do ranqueamento, como também multas e penalidades da própria organização por desrespeito às suas normas.

A legislação europeia prevê, ainda, em seu artigo 46, a obrigatoriedade de apresentação de garantia por parte do responsável pelo tratamento para que seja possível operar a transferência internacional de dados quando não há decisão tomada pela comissão. Essa garantia pode ser na forma de um instrumento vinculativo e com força executiva entre autoridades ou organismos públicos. Imagina-se que para o caso da organização, adapta-se essa norma com a obrigatoriedade desse título ser executável no país de origem do usuário.

Deve ter também um código de conduta, que é aprovado e demonstrado quando da certificação a ser entregue pela organização internacional. Esse código de conduta é um dos pressupostos para a transferência internacional dos dados, bem como para a certificação que será abordada quando se falar das empresas que atuam na internet e seu papel na organização.

Essas garantias também podem se dar, pela legislação europeia, por meio de disposições contratuais entre os responsáveis pelo tratamento e os destinatários dos dados no país terceiro ou organização internacionais, bem como disposições a inserir nos acordos administrativos entre as autoridades ou organismos públicos que contemplem os direitos oponíveis dos titulares dos dados.

A transferência internacional dos dados é um dos principais aspectos de atenção que a organização hipotética precisa se atentar. Ela é quem deve, no mundo, ser responsável pela fiscalização dessa transferência. Afinal, é a transferência de dados que pode levar aos problemas e conflitos anteriormente abordados. Ela é que pode levar determinado usuário a ter seus dados explorados longe de seu alcance, assim pode fazer com que duas jurisdições distintas tratem o mesmo dado com dois

sistemas regulatórios diferentes. As regras a serem adotadas pela organização devem ser inspiradas na legislação europeia, que aborda a questão de forma mais completa quanto possível no atual momento. Ela cria a proteção ao usuário de ver seus direitos resguardados e a certeza que será tratado com o mesmo respeito para onde o dado for levado. Esse é o objetivo das regras criadas pela GDPR para a transferência internacional dos dados, bem como é um dos objetivos da criação da hipotética organização.

6.2 A PARTICIPAÇÃO DE ATORES PRIVADOS NA ORGANIZAÇÃO

Como dito anteriormente, pretende-se que a organização internacional para a proteção de dados pessoais conte em seus quadros com membros da sociedade civil, bem como representação das empresas que trabalham na internet e que operam diariamente com o processamento de dados como forma do seu modelo de negócios. A esses membros, deve ser dado direito a voto.

Porém, há também um impossível número de indivíduos que utilizam a internet, não sendo possível entregar direito a voto a cada um dos representantes de cada uma das empresas individualmente. Assim, faz-se necessário que dentro da organização exista representação desses atores, seja por meio de entidades não governamentais para representar a sociedade civil, seja por grupos organizados de empresas do setor. A participação dessas entidades representantes deve ser aprovada pela assembleia geral da organização. Porém, os Estados membros não podem participar da formação desses grupos, para que sejam legítimos representantes dos interesses daqueles que eles defendem.

Em se tratando de uma tentativa de solução para o problema da falta de respeito aos direitos dos usuários quando transferidos os dados internacionalmente por empresas, a participação ampliada é um dos pilares mais importantes para o estabelecimento da hipótese da organização internacional como um instrumento de governança global.

6.2.1 As empresas da internet

Além do direito a voto no estabelecimento das normas para a proteção de dados, é preciso buscar meios de se fazer vantajoso para as empresas da internet fazer parte da organização. Isso, inclusive, seria uma forma de promover a proteção por meio das empresas que atuam no ambiente digital.

Assim, a organização pretende ser uma forma de fomento de sustentabilidade empresarial no sentido de respeito aos direitos dos usuários. Neste sentido, a identificação e o diálogo com os diversos atores são peças-chave para atingir a sustentabilidade corporativa. Para a integração dos sistemas de gestão visando a sustentabilidade, é necessário compreender os interesses e as percepções do setor empresarial (LAURIANO, 2012, p. 4).

Para trazer eficácia para a atuação da organização perante as empresas, aquelas que integram o grupo pertencente à organização serão detentoras de um selo especial. Este selo terá o condão de demonstrar que a empresa em questão atua em conformidade com as diretrizes legais estabelecidas. Trata-se de um sistema parecido com o que é usado na governança ambiental global.

Como destacam Gonçalves e Fontoura (2011, p. 53), o sucesso das empresas depende cada vez mais da imagem e da ação efetiva em questões ambientais, em que se buscam selos de aprovação referentes à origem de seus produtos, bem como a construção de uma imagem positiva de responsabilidade social perante as comunidades e o mercado. Além disso, destaca-se a busca pela aprovação de certificados da International Organization for Standardization (ISO).

Este é o escopo que pretende se dar para o selo a ser disponibilizado pela organização. Busca-se um *ISO da Proteção de dados pessoais*. Assim, as empresas têm um benefício à sua imagem perante os usuários. Busca alimentar a necessidade das empresas gigantes da internet em demonstrar uma responsabilidade social no processamento dos dados pessoais, bastante impactadas com os recentes casos envolvendo *Facebook*, por exemplo.

Então, detectado que essas empresas detentoras do selo fazem uso dos dados pessoais fora de conformidade com as regras da organização, elas sofrerão sanções, desde a perda do selo, perda do direito de participação do processo de decisão, até multas pecuniárias pagas à organização. Para dar maior legitimidade e eficácia às sanções impostas que se faz tão necessária a participação ativa das empresas no

processo de decisão da organização. Toda regra a ser aplicada deve passar pelo consenso também dessas empresas.

É válido lembrar que a LGPD brasileira, em seu artigo 33, inciso II, alínea d, determina que a transferência internacional de dados poderá se dar mediante comprovação por selos e certificados de conduta emitidos que atestem que o país, organismo internacional que está requerendo o dado, está de acordo com as mesmas proteções. A organização proposta pode ser a responsável por este selo.

A GDPR trata desse assunto no artigo 42. Nesse artigo, consta que os Estados membros e outros entes especializados devem criar procedimentos de certificação em matéria de proteção de dados. Assim, os atores presentes na União Europeia têm a obrigação de criar selos e marcas de comprovação da conformidade da proteção de dados pessoais e das operações de tratamento responsável e dos subcontratantes com a legislação. Abre-se apenas a concessão de necessidades específicas para pequenas e médias empresas.

Esses selos ou marcas são estabelecidos para comprovação das garantias adequadas fornecidas pelos responsáveis pelo tratamento e seus subcontratantes que não estão situados em território europeu. Essa certificação prevista é voluntária e não é capaz de diminuir as responsabilidades que advém do processamento de dados. Sua certificação é emitida por organismos previstos na própria GDPR. Trata-se do *Selo Europeu de Proteção de Dados*.

Para receber esse selo, é preciso que os responsáveis ou subcontratantes abram o tratamento de dados para avaliação da União Europeia, como todo acesso às atividades de tratamento e toda a informação que haja necessidade para efetuar o procedimento da certificação. A lei também define um período máximo de certificação por três anos, podendo ser renovado se apresentada as mesmas condições, e é perdida a certificação caso os requisitos não sejam mais encontrados. Esses selos são públicos e o comitê especializado da União Europeia é obrigado a disponibilizá-los.

Da mesma forma, essa é uma das principais atuações que a organização proposta por esse trabalho deve ter. Ela precisa ter departamentos específicos para a certificação dos atores da internet, não com escala regional como o selo europeu, mas em escala global. Da mesma forma, é preciso que a organização tenha um comitê para criação desse selo de conformidade com as regras da organização.

Para as empresas que atuam na internet, pode haver interesse em certificação de conformidade com as regras da organização. Esse selo pode ser cobrado para ajudar a tornar a organização viável, mas é importante que a concessão do selo não possa ser irrestrita e vinculada apenas ao pagamento de determinada mensalidade. O pagamento de valores para requisição do selo não pode consignar imediatamente o recebimento deste. O selo deve vir apenas com a conformidade das regras de definidas, de forma objetiva.

Essa certificação também não será a prova absoluta para eximir a responsabilidade caso um ator ou seu subcontratado venha a cometer alguma lesão ao direito de algum usuário. Inclusive, uma das penas para o descumprimento das regras deve ser a perda do selo pago.

Por fim, as empresas da internet devem manter completa transparência quanto ao processamento de dados para com os fiscais da organização. Esses fiscais não podem ser fechados apenas na sede da organização, ela precisa ter uma atuação global espalhada por todo mundo. Para isso, o financiamento por meio do pagamento das empresas pelo selo é fundamental. Mesmo para que os usuários possam ter suas reinvindicações atendidas, uma atuação próxima de empresas locais pode ser crucial.

Também, para o selo ser viável e para a fixação de um valor mensal a ser cobrado de empresas, deve ser levado em consideração o tamanho da empresa. Um selo impossível de ser comprado por *start-ups*, por exemplo, é um selo que não atinge sua finalidade no atual cenário empresarial. Também é preciso ajustar um prazo para a validade do selo. Os três anos da legislação europeia são um tempo razoável.

6.2.2 A representação dos usuários

Como dito anteriormente, a princípio, na assembleia geral, a participação da sociedade civil deve se dar por meio de organizações não governamentais, sejam elas de cunho acadêmico ou de proteção dos interesses do cidadão. Da mesma forma, para ingressarem na organização, estas precisam ser aprovadas pela assembleia e obedecer aos requisitos que devem ser definidos no instrumento constitutivo da organização. Porém, isso vale no que se refere ao direito de voto perante a definição dos regulamentos da organização.

Para o usuário, pessoa física ou jurídica, mas nacional de determinado Estado, que tenha alguma demanda para tratar que verse sobre a proteção de dados pessoais, a organização deverá criar um mecanismo para receber essas demandas. Deve ser criado um instrumento para peticionamento online de questões envolvendo o processamento de dados pessoais diretamente do usuário para a organização, via on-line. Esse peticionamento deverá resultar em esclarecimento por parte das empresas, ou Estado, que fazem parte da organização e que detém seu selo de aprovação, e irá ter como consequência um relatório. Caso nesse relatório não conste uma utilização adequada dos dados pessoais, aquele que processou os dados deverá sofrer as penalidades internas da organização, com multas e/ou perda do selo de aprovação. Esse relatório poderá ser usado pelo indivíduo para buscar alguma solução pela via judicial de seu país, fazendo uso dos serviços de cooperação entre jurisdições caso seja necessário.

Cabe ressaltar que não se tenta ter um instrumento judicial dentro da organização. Não se trata de um tribunal para proteção de dados. É um instrumento fiscalizatório do processamento de dados dentro dos parâmetros estabelecidos pela organização, sendo que o seu parecer será técnico, não jurídico. Não irá condenar para uma indenização ao usuário, mas, produzirá prova técnica do fato, com recomendação de jurisdição adequada. Punirá internamente com os seus mecanismos, selos, índices, restrições e multas, os infratores. Essas multas se revertem para a própria organização para, assim, desmotivar o cometimento de novas infrações, ao mesmo tempo em que promove o sustento da própria.

7 CONCLUSÃO

A presente dissertação teve por objetivo apresentar a hipótese de uma organização internacional com o objetivo de promover o direito de proteção de dados pessoais. Isso porque, com a criação de legislações nacionais para resolver a questão com a internet global, alguns problemas são levantados: Como as novas leis de proteção de dados pessoais, criadas por legislações nacionais ou com jurisdição territorialmente limitada, podem dar conta de solucionar com eficácia o processamento de dados na internet, que é global por natureza? Como fica a proteção de usuários de localidades que ainda não têm tais legislações, uma vez que se trata de um direito de todos? Por fim, como garantir que essa proteção seja uniforme em todos os lugares, para todos os usuários, sem criação de fronteiras digitais ou paraísos para o processamento dos dados?

Assim, primeiramente demonstram-se as características da internet que demonstram o determinado levantado pela dissertação. Para demonstrar tal hipótese, se utiliza do método hipotético dedutivo e a pesquisa referencial bibliográfica.

A primeira dessas características é a extraterritorialidade. A internet está presente em todos os lugares do mundo ao mesmo tempo. Ela permite comunicação simultânea entre qualquer um que esteja conectado a ela, independente de qual canto do planeta eles estejam. A maioria das pessoas já tem acesso à internet, em especial, nos países desenvolvidos. Isso é a internet. Uma rede mundial de computadores que permite a troca de dados, informações e conexões em qualquer lugar. Porém, permitir a relação entre pessoas, seja comercial, emocional ou de qualquer outra natureza, tem grande possibilidade de gerar conflitos.

A segunda característica que é apontada como relevante para o problema da dissertação é que a internet foi arquitetada e tem um desequilíbrio de poder entre seus atores. Grande parte do poder na internet está em mãos de companhias privadas, que detêm uma quantidade gigantesca de dados sobre os usuários de seus serviços.

Essas empresas que dominam uma enorme quantidade de dados criaram modelo de negócio revolucionário. Elas operam essa enorme quantidade de dados em todo o mundo, movendo os dados pelo mundo todo sem os usuários terem como saber o que está sendo processado em sua totalidade. Os usuários entregam seus dados para essas empresas para que tenham acesso a seus serviços de forma

gratuita. Então, com base nos dados coletados, as empresas vendem espaços publicitários direcionados a esses indivíduos. Assim, se tem formado um modelo econômico baseado na vigilância, na coleta, processamento e venda dessas informações.

Essas características criaram desafios para as legislações. Desafios que não existiam quando os conceitos de soberania nacional foram desenvolvidos. A razão disso é que a característica de extraterritorialidade da internet cria situações que os poderes soberanos, ao se chocarem diante de um conflito, irão atuar de acordo com interesses nacionais. Assim, existe ou deixa de existir cooperação entre as jurisdições por conveniência.

Leva-se a conclusão de que a internet depende de uma solução jurídica que tenha uma característica global. Isso não é menos verdade para a proteção de dados pessoais. Quando esses dados atravessam as fronteiras de forma instantânea, uma solução jurídica para conflitos que podem surgir no processamento desses dados deve ser uma solução global. Sob o risco de se repetir os casos elencados no capítulo três, em que a prestação jurisdicional não é satisfeita.

Para se aproximar mais do tema, o capítulo quatro fala em especial da proteção de dados pessoais. A conclusão que se apresenta é o direito de proteção de dados pessoal vista como um direito da personalidade, um direito fundamental em alguns Estados e um direito humano para todos. Apesar de sua correlação importante com o direito da privacidade, a proteção de dados pessoais evolui de forma autônoma e está além da relação entre apenas o que deve ser tratado como público ou privado. O principal aspecto da proteção de dados pessoais que não conversa com o direito da privacidade é o direito de exigir a correção de dados, sem que isso importe se esse dado pode ou não ser privado.

O quinto capítulo teve por objetivo mostrar como as legislações de dados pessoais tem tratado a internet global. São apresentadas duas perspectivas. A primeira é a perspectiva adotada pela União Europeia e a segunda é a Chinesa. A União Europeia, seguida pelo Brasil e outros países, adotou um sistema de princípios de dar o controle de seu dado ao usuário e a responsabilidade sobre as consequências nas organizações que o processam, a depender do impacto deste nos usuários. Essas legislações apresentam soluções para a extraterritorialidade, criando obrigações que tentam dar eficácia para as decisões sobre os dados pessoais dos

indivíduos localizados nesses territórios. Apesar de ser o melhor sistema, com a maior evolução nos direitos dos indivíduos que utilizam a internet, questiona-se se os problemas apontados no capítulo três seriam resolvidos. Também não apresenta solução para o direito de forma global, fora dos Estados que essas legislações abordam.

A segunda perspectiva é de uma internet fechada, repleta de fronteiras. Além de como redes nacionais permitiriam governos atuarem de forma muito perigosa no controle de comportamento da população, seria um passo atrás na globalização.

Por todo o exposto na dissertação, apresentamos a hipótese de uma organização internacional para a proteção de dados pessoais. Essa organização internacional tem um sistema global, atuando no mundo todo, resolvendo a questão da extraterritorialidade. As empresas devem fazer parte da organização, devido a sua relevância para o ambiente digital, respeitando também os benefícios da economia com base em dados, contendo seus lados negativos. Ela tem meios de comunicação entre jurisdições para evitar os conflitos do segundo capítulo. Ela pretende espalhar o direito por todo o mundo de forma uniforme, por ser um direito humano. Por fim, atendendo ao capítulo cinco, ela tem como molde para a proteção a legislação europeia.

Como características da organização, ela teria personalidade jurídica própria para cumprir seu objetivo, alcance global e vocação específica para a promoção da proteção de dados pessoais. Sua assembleia geral irá definir uma legislação adequada para o direito de proteção de dados pessoais, a princípio, inspirado na legislação europeia. Porém, é importante dar direito de participar da discussão as empresas da internet bem como as organizações representantes da sociedade civil. Assim, representa uma solução de governança global, com participação ampliada e fora das tradicionais formatações hierárquicas.

Aos Estados ingressantes, existirá a obrigação de internacionalizar as normas acertadas na organização. Bem como também existirá um sistema interestatal de cooperação jurisdicional. Onde existirá um órgão da atividade que irá ser responsável por definir questões de conflitos de jurisdição ou a transferência de dados a pedido de judiciários nacionais. Não se trata de um órgão jurisdicional, mas um órgão técnico que irá fiscalizar a proteção de dados pessoais no mundo.

É importante a participação de entidades privadas. Empresas e sociedade civil. Para as empresas, a criação de um selo de cumprimento com as normas da organização é o estímulo para o ingresso. Este selo será fiscalizado pela organização, que poderá retirar o selo ou punir com multas o descumprimento. Para o indivíduo, deverá haver um sistema de peticionamento, no qual será feito um relatório pela autoridade fiscalizadora, que poderá aplicar as punições já referidas. A participação de organizações não governamentais nas decisões da organização também é vital para o seu bom funcionamento.

Assim, a organização se apresenta como única solução para atender todos os questionamentos apresentados por esta dissertação.

REFERÊNCIAS

ALMEIDA, Marília. **Veja quem são os mais ricos do mundo em 2019, segundo a Forbes**. Exame. 2019. Disponível em https://exame.abril.com.br/negocios/veja-quem-sao-os-mais-ricos-do-mundo-em-2019-segundo-a-forbes/ Acesso em: 11 de out. de 2019.

ARGA E LIMA, Francisco. CARVALHO, Matheus Magalhães de. **O direito de apagamento de dados como uma realidade global.** Anuário da Proteção de Dados 2019. CEDIS, Centro de I&D sobre Direito e Sociedade. Universidade Nova de Lisboa. Lisboa. 2019.

BBC. **Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades.** 20/03/2018. Disponível em https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml Acesso em: 14 de dez. de 2020.

BIERMANN, Frank. PATTBERG, Philipp. **Global Environmental Governance Revisited**. Cambridge, The MIT Press, 2012.

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

BOFF, Salete Oro. FORTES, Vinícius Borges. **Internet e Proteção de Dados Pessoais: Uma Análise das normas jurídicas brasileiras a partir das repercussões do caso NSA vs. Edward Snowden.** Cadernos do Programa de Pós Graduação em Direito/UFRGS. Volume 11. Nº 1. Porto Alegre. 2016.

BOLLEN, Johan. HUINA, Mao. XIAOUN, Zeng. **Twitter mood predicts the stock market**. Journal of Computational Science 2, no. 1 (2011): 1-8. Disponível em: http://www.ccs.neu.edu/home/amislove/twittermood/. Acesso em: 16 de abr. de 2019.

BRASIL. **Constituição da República Federativa do Brasil, de 05 de outubro de 1988**. Brasília, DF: Assembleia Nacional Constituinte. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 14 de fev. de 2020.

_____. **Lei nº 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Brasília. DF. Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 14 de fev. de 2020.

_____. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília. DF. Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 18 de fev. de 2020.

CASTELLS, Manuel. **A Sociedade em Rede: A era da informação: economia, sociedade e cultura.** V1. Editora Paz e Terra. São Paulo. 2011.

CERDA, Alberto. **Chilean Bill on personal data protection is a setback for people and business.** Digital Rights: Latin America and the Caribbean / [Editor] Eduardo Magrani. Rio de Janeiro. Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas. 2017.

COSTA, Ramon Silva. OLIVEIRA, Samuel Rodrigues de. **Os direitos da personalidade frente à sociedade de vigilância: privacidade, proteção de dados pessoais e consentimento nas redes sociais.** Revista Brasileira de Direito Civil em Perspectiva. V. 5. N. 2. Belém. 2019.

DÍAS, Marianne. **Your fingerprint for a kilogram of flour: biometric and privacy in Venezuela.** Digital Rights: Latin America and the Caribbean / [Editor] Eduardo Magrani. Rio de Janeiro. Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas. 2017.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro. Volume 1**. São Paulo. Saraiva. 2004.

DIXON, Helen. **Regulate to Liberate**. Can Europe Save the Internet?. New York: Foreign Affairs. September 19, 2018.

DOMINO, Jenny. **Gambia v. Facebook: What the Discovery Request Reveals about Facebook's Content Moderation**. Just Security. 6/06/2020. Disponível em: https://www.justsecurity.org/71157/gambia-v-facebook-what-the-discovery-request-reveals-about-facebooks-content-moderation/ Acesso em: 02 de nov. de 2020.

FACEBOOK, INC, **Termos de Serviço**. 2018. Disponível em https://www.facebook.com/terms Acesso em: 18 de jul. de 2019.

FREIRE E ALMEIDA, Daniel. **O Poder Judicial Nacional e os Desafios da Internet Global**. Os Conflitos Jurisdicionais Digitais na Internet Global. New York. Lawinter Editions. 2019.

FREIRE E ALMEIDA. Daniel. **Um Tribunal Internacional para a Internet**. São Paulo. Almedina. 2015.

G1. **Facebook eleva para 87 milhões nº de usuários que tiveram dados explorados pela Cambridge Analytica.** 04/04/2018. Disponível em https://g1.globo.com/economia/tecnologia/noticia/facebook-eleva-para-87-milhoes-o-n-de-usuarios-que-tiveram-dados-explorados-pela-cambridge-analytica.ghtml Acessado em: 14 de dez. de 2020.

GONÇALVES, Alcindo Fernandes. FONTOURA, José Augusto. **Governança Global e regimes internacionais**. São Paulo, Almedina, 2011.

GONÇALVES, Caros Roberto. **Direito Civil esquematizado v. 1 3. Ed. Ver. E atual**. São Paulo. Saraiva. 2013.

GOOGLE, INC. **Termos de Serviço do Google**. 2017. Disponível em https://policies.google.com/terms?hl=pt-BR Acesso em: 18 de jul. de 2019.

GUIDI, Guilherme Berti de Campos. **O Papel do Consentimento Para a Proteção de Dados Pessoais: União Europeia, Estados Unidos e Brasil**. Direito Internacional em Expansão. Volume XVI. Belo Horizonte. Arraes Editores. 2019.

GUIDI, Guilherme Berti de Campos. **Modelos Regulatórios de Proteção de Dados.** Privacidade em Perspectiva. Rio de Janeiro. Livraria e Editora Lumen Juris. 2018.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTAÍSTICA, PNAD Contínua TIC 2017: **Internet chega a três em cada quatro domicílios do país, 2018**. Disponível em https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/23445-pnad-continua-tic-2017-internet-chega-a-tres-em-cada-quatro-domicilios-do-pais Acesso em 28/07/2019.

INTERNET WORLD STATS. **Internet Usage Statistics**. The Internet Big Picture. 2019. Disponível em https://www.internetworldstats.com/stats.htm. Acesso em: 05 de out. de 2019.

JURCYS, Paul. DONEWALD, Chris. GLOBOCNIK, Jure. LAMPINEN, Markus. **My Data, My Terms: A proposal for Personal Data Use Licenses.** Harvard Journal of Law & Technology. Volume 33. Digest Spring. 2020.

KOBIE, Natalie. **The Complicated truth about China's social credit system.** *Wired*, London, 05 Jun. 2018. Disponível em: https://www.wired.co.uk/article/china-social-credit-system-explained . Acesso em: 29 de out. de 2020.

LAURIANO, L. **Rumo à integração da sustentabilidade no sistema de gestão empresarial**. 2012.

LESSIG, Lawrence. **Code: Version 2.0**. New York.: Basic Books. 2006.

LOPES, Gills Vilar. **Vigilância Cibernética no Brasil: O Caso Sob o PRISMa de um *insider*.** Revista Eco Pós. Tecnopolíticas e vigilância. V. 18. Rio de Janeiro. 2015.

MAYER-SCHÖNBERGER, Viktor, RAMGE, Thomas. **A Big Choice for Big Tech. Share Data or Suffer the Consequences**. New York: Foreign Affairs. September 19, 2018.

MILANÉS, Valeria. **Personal Data, companies and the cloud: are we ready for it?** Digital Rights: Latin America and the Caribbean / [Editor] Eduardo Magrani. Rio de Janeiro. Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas. 2017.

ORGANIZAÇÕES DAS NAÇÕES UNIDAS. **Oral Revisions of 30 June. 2016**. Disponível em: https://www.article19.org/data/files/Internet_Statement_Adopted.pdf Acesso em: 06 de nov. de 2018.

PALIN, Megan. **China's 'social credit' system is a real-life 'Black Mirror' nighmare.** *NY Post*, New York, 19 Set. 2018. Disponível em:

https://nypost.com/2018/09/19/chinas-social-credit-system-is-a-real-life-black-mirror-nightmare/. Acesso em: 20 de out. de 2020.

PECK, Patrícia. ROCHA, Henrique. **Advocacia digital**. São Paulo. Thomson Reuters. 2018.

PEREIRA, Francisco José Rocha. **A General Data Protection Regulation (GDPR) e sua influência na elaboração da Lei Geral de Proteção de Dados (LGPD) brasileira**. Proteção de dados na perspectiva do direito internacional na internet. Lawinter Editions. New York. 2019.

PINHEIRO, Patricia Peck. **Direito digital** / **Patricia Peck Pinheiro. — 5. ed. rev., atual. e ampl. de acordo com as Leis n. 12.735 e 12.737, de 2012**. São Paulo. Saraiva. 2013.

PRIVACY INTERNATIONAL. **The Keys to Data Protection: A guide for policy engagement on Data Protection**. 2018. Disponível em: https://privacyinternational.org/data-protection-guide. Acesso em: 07 de nov. de 2018.

REIDENBERG, Joel. R. **The Yahoo! case and the international Democratization of the Internet** – Joel R. Reidenberg – disponível em: http://papers.ssnr.com/paper.taf?abstract_id=267148 Acesso em: 07 de jul. de 2019.

REZEK, José Francisco. **Direito Internacional Público: Curso Elementar** – 12 Ed. rev. e atual. – São Paulo, Saraiva, 2010

SEGAL, Adam. **When China Rules the Web**. Foreign Affairs, New York, September 19, New York: Foreign Affairs. September 19, 2018.

SHAW, Malcolm N., **International Law, Sixth Edition**. Nova York. Cambridge University Press. 2008.

SHERWIN, Emily. **Rússia quer se desconectar da internet global**. DW. 12/02/2019. Disponível em https://p.dw.com/p/3DFJf Acesso em: 20 de ago. de 2019.

SILVA, Arthur Marques. **Poder Virtual: quem comanda a Internet**. Os Conflitos Jurisdicionais Digitais na Internet Global. Lawinter Editions. New York. 2019.

TRENTIN, Taise Rabelo Dutra. TRENTIN, Sandro Seixas. **Internet: Publicações Ofensivas em Redes Sociais e o Direito à Indenização Por Danos Morais.** Revista Direitos Emergentes na Sociedade Global v1 n1. Universidade Federal de Santa Maria. 2012. Santa Maria/RS. Disponível em: https://periodicos.ufsm.br/REDESG/article/view/6263/pdf#.X5sn34hKjIU Acesso em: 29 de out. de 2020.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. **Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González**. 2014. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131. Acesso em: 18 de jul. de 2019.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do parlamento europeu e do conselho de 27 de abril de 2016.** Relativo à proteção de dados pessoais singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (regulamento geral de proteção de dados). Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT . Acesso em: 24 de abr. de 2020.

VERNIK, Esteban. **As Nações, o imperialismo e a circulação do segredo: algumas reflexões sobre o caso Snowden.** Revista Brasileira de Estudo de Defesa. Ano 1. Nº 1. Jul/dez. 2014.

VOIVODIC, Maurício de Almeida. **Os desafios de legitimidade em sistemas multissetoriais de governança: uma análise do Forest Stewardship Council.** Disponível em: https://teses.usp.br/teses/disponiveis/90/90131/tde-12082011-095921/pt-br.php. Acesso em: 06 de dez. de 2020.