I ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

DANIELLE JACON AYRES PINTO

AIRES JOSE ROVER

FABIANO HARTMANN PEIXOTO

D597

Direito, governança e novas tecnologias I [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Danielle Jacon Ayres Pinto

Aires Jose Rover

Fabiano Hartmann Peixoto – Florianópolis: CONPEDI, 2020.

Inclui bibliografia

ISBN: 978-65-5648-078-7

Modo de acesso: www.conpedi.org.br em publicações

Tema: Constituição, cidades e crise

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Assistência. 3. Isonomia. I Encontro Virtual do CONPEDI (1: 2020 : Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

I ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

Apresentação

O I ENCONTRO VIRTUAL DO CONPEDI, ocorrido entre os dias 23 e 30 de junho de 2020, foi realizado exclusivamente a partir da utilização das novas tecnologias de informação e comunicação. Foi o maior sucesso nesses tempos de pandemia. Mais do que nunca se viu a tecnologia servindo como instrumento de ação no campo do conhecimento e da aprendizagem, o que este GT sempre defendeu e esteve atento discutindo os limites e vantagens dessa utilização. Os artigos apresentados, como não podia deixar de ser, mostraram que os temas relacionados às novas tecnologias estão cada vez mais inseridos na realidade jurídica brasileira e mundial. Diversos fenômenos do cenário digital foram abordados ao longo dos trabalhos e demonstraram que a busca por soluções nessa esfera só pode ser pensada de forma multidisciplinar.

Assim, vejamos as principais temáticas tratadas, em sua sequência de apresentação no sumário e apresentação no GT. No primeiro bloco temático temos:

• Lei geral de proteção de dados

• proteção da intimidade, privacidade e aos dados sensíveis dos empregados

• anonimização e pseudoanonimização dos dados pessoais

• monetização de dados pessoais na economia informacional

• modelos regionais de obtenção de dados em aplicações na internet

• problemática dos brinquedos conectados

No segundo bloco:

• inteligência artificial e uma justiça preditiva

• neurociências no brexit

• confiança em sistemas de inteligência artificial

• chatbot, normas do bacen e fintechs de crédito

No terceiro bloco:

• internet como ferramenta de participação

• deliberação democrática digital

• ressocialização digital dos idosos

• gestão pública sustentável

• governança eletrônica na administração pública brasileira

• teoria do processo na era digital

No quarto e último bloco:

• a tecnologia e o princípio do contraditório

• vulnerabilidade aos cibercrimes

• fakenews

• pandemia e telemedicina

• pagamentos instantâneos e transações eletrônicas bancárias via whatsapp

Com esses estudos de excelência os coordenadores desse grupo de trabalho convidam a todos para a leitura na integra dos artigos.

Aires José Rover – UFSC

Fabiano Hartmann Peixoto - Universidade de Brasília

Danielle Jacon Ayres Pinto – IMM/ECEME e UFSC

Nota técnica: Os artigos do Grupo de Trabalho Direito, Governança e Novas Tecnologias I apresentados no I Encontro Virtual do CONPEDI e que não constam nestes Anais, foram selecionados para publicação na Plataforma Index Law Journals (https://www.indexlaw.org/), conforme previsto no item 8.1 do edital do Evento, e podem ser encontrados na Revista de Direito, Governança e Novas Tecnologias. Equipe Editorial Index Law Journal - publicacao@conpedi.org.br.

MODELOS REGIONAIS DE OBTENÇÃO DE DADOS EM APLICAÇÕES NA INTERNET: APLICABILIDADE SEGUNDO A LEGALIDADE E ISONOMIA DE PLAYERS EM PLATAFORMAS DIGITAIS

REGIONAL MODELS FOR GATHERING DATA IN INTERNET APPLICATIONS: APPLICABILITY ACCORDING TO THE LEGALITY AND ISONOMY OF PLAYERS ON DIGITAL PLATFORMS.

Ricardo Bravo [1]
Tamara Rodrigues Ramos [2]

Resumo

A Internet e o uso de tecnologias de comunicação digitais representam imensos avanços para a democracia como pluralidade de fontes e maior possibilidade de manifestação, bem como meio precípuo para obtenção de serviços e informações. Todavia, também representa desafios ao Estado em diversos aspectos, particularmente isonomia, antitruste, e obtenção de dados. Indica-se que há diversos modelos ou formas de tratamento de dados e que estas estão relacionadas com particularidades e interesses de países e sociedades diversas, com destaque para os modelos norte-americano, chinês e europeu, que podem orientar escolhas nacionais.

Palavras-chave: Obtenção de informações, Proteção da dados, China/eua/europa

Abstract/Resumen/Résumé

The Internet and the use of digital communication technologies represent immense advances for democracy as a plurality of sources and greater possibility of manifestation, as well as a primary means of obtaining services and information. However, it also represents challenges to the State in several aspects, particularly isonomy, antitrust, and data collection. It is indicated that there are several models or forms of data processing and that these are related to the particularities and interests of different countries and societies, with emphasis on the US, Chinese and European models, which can guide national choices.

Keywords/Palabras-claves/Mots-clés: Data gathering, Data protection, China/usa/europe

[1] Mestre em ciências pelo ITA, Mestre em Direito pelo IDP e UniCeub, doutorando em ambas as instituições, registrador de imóveis no ES.

[2] Mestre em Direito pelo UniCeub, mestranda em Direito pela Universidade Autônoma de Lisboa, advogada.

1 INTRODUÇÃO

Um tema relevante no direito privado é a redefinição de limites e parâmetros para a distinção entre público e privado com a disseminação de tecnologias que tornam ubíquo o acesso a diversas fontes de dados, como produtores e consumidores por meio da popularização de internet, celulares aplicativos e formas de compartilhamento. Nesse contexto, parcela grande dos dados produzidos é criado, armazenado, tratado ou disponibilizado por plataformas associadas a entidades privadas, o que inclui dados que os usuários cedem a empresas por meio de aceitação de termos de usos como forma de acesso a um serviço tal como rede social, busca, sistema operacional de um celular como também a partir de integrações autorizados por lei.

Nesse sentido, mesmo que parcela relevante dos dados passem por entes privados e se refiram a questões privadas, o Estado mostra interesse em obter tais informações. Nesse sentido, o acesso a dados de uso de internet na forma que podem ser adequados a persecuções criminais, questões tributárias e outras tais como administração da justiça, mas representa um desafio à estrutura jurídica e administrativa do Estado em diversos aspectos.

A epidemia do novo coronavírus evidenciou que dados de localização e dados privados em geral de pessoas podem ser úteis para fins de saúde pública, para buscar padrões, ou para verificar o cumprimento de isolamento.

Os desafios ocorrem porque a estrutura da internet não tem como objetivo precípuo fornecer dados para o Estado, e na forma que este desejaria, mas, ao contrário, possui mecanismos que se bem implementados afastam justamente a possibilidade de obter dados *ad hoc*. Por exemplo, há camadas de interação nas redes e de aplicação, provedores de comunicação, provedores de serviço, de conteúdo com relativa independência entre si, os dados podem ser facilmente armazenados em mais de um país (datacenter). Por exemplo, a linha telefônica comutada tradicional é uma peneira em que os dados podem vazar ou ser coletados com facilidade. Já aplicativos de comunicação como *whatsapp*, podem se valer de vários mecanismos como criptografia ou validação de identidades. Isso significa que o Estado pode ter que recorrer à empresa responsável para tentar obter informações, e, se esta implementou bem aquilo que se propôs eventualmente até mesmo por um “end user license agreement”, fornecer os dados completos seria um atestado de incompetência.

É nesse ponto que o papel do Estado deve ser revisto. A obtenção de simples dados sobre o conteúdo e sobre comunicação requer uma previsão legal ou regulamentação prévia e num nível

técnico e regulatório adequado, tanto no sentido de envolver idiossincrasias como no sentido de não gerar tratamentos privilegiados ou discriminatórios. Há também a questão da multiplicidade de jurisdições e interesses, algo que a cooperação pode reduzir, mas não eliminar o problema.

2 DESAFIOS PARA O ESTADO NACIONAL

O sistema jurídico estruturado com base no estado nacional tinha o condão de reduzir complexidades, estabilizar expectativas e propiciar um ordenamento jurídico que fosse eficaz dentro da jurisdição. Como indica o sociólogo alemão Niklas Luhmann (1996, p. 299), que foi também um dos primeiros a analisar o sistema internacional do direito, em que não há um órgão político semelhante ao que há nas esferas nacionais, e profetiza que eventualmente a história mostrará que o modelo dos estados nacionais não passa de algo copiado da Europa do século XIX, datado, que pode ser mostrar inadequado.

A Internet e as comunicações digitais fizeram a previsão de que o sistema jurídico baseado em estados nacionais apresenta dificuldades para tratar algumas situações tenha se concretizada de forma mais incisiva. Por exemplo, as linhas de telefonia fixa são circuitos comutados e exclusivos, que são, de certa foram, propícios e feitos para que a comunicação seja violada. Assim, se havia uma ordem judicial que determine a quebra do sigilo telemático, bastava a colocação de dispositivo físico na rede de telefonia e tudo pronto. O mesmo não se pode dizer da comunicação via sites ou aplicativos no topo de camadas de comunicação com o *Whatsapp*. Mesmo que haja uma ordem judicial determinando a captura de informações, caso a empresa controladora mantenha os termos da licença de usuário e faça uma implementação adequada dos protocolos, torna-se inviável a devassa. Nesse cenário, que existe na Arguição de descumprimento de preceito fundamental (ADPF) 403, o Poder Judiciário deve aceitar que existe uma limitação à bisbilhotice estatal ou que os requisitos devem ser estabelecidos *a priori*, como forma de regulação.

Existem outros mecanismos pelos quais o modelo de rede aberta propicia abstrações e camadas com diferentes atribuições[1] em diversos níveis, com pacotes que podem transitar por fibras ópticas, cabos de cobre ou ondas eletromagnéticas no nível físico e uma miríade de aplicações em outras camadas. Com o aumento de banda disponível, capacidade de transmitir informações

[1] No sentido do modelo teórico de camadas em sistemas interconectados. (TANENBAUM, 2011) e no sentido de fato das camadas do protocolo IP (*internet protocol*).

por unidade de tempo, e a redução de latência, o seja, o tempo respostas entre nós de rede, aumento da capacidade computacional e de armazenar energia, redução de tamanho de componentes e aumento de capacidade e poder de processamento, cria-se um ambiente propício para inovação e adição de funcionalidades diretas e outras ligadas a qualidades ou não funcionais.

A rede passa a ser vista como um bem público, fator de crescimento econômico e inovação, e passa a ser fundamental que eventual regulação preserve a isonomia dos participantes e janelas de inovação. O Estado em si se beneficia de tais elementos, e passa a ser um agente que pode ser valer de vantagens, mas também se condiciona a limites. Obviamente, no extremo o Estado poderia censurar ou bloquear todos os sites de outro país, ou banir um site como um todo, mas isso seria viável num contexto não democrático ou razoável, assim como afetaria vários direitos fundamentais dos banidos ou de usuários. Ressalta-se que mesmo um bloqueio como o indicado não é algo tecnicamente simples. Menciona-se o uso de *proxies*, virtualizações, mas principalmente que se o país necessita se comunicar com outros por meio digitais, não é tecnicamente viável bisbilhotar todas as comunicações justamente porque possuem camadas como criptografia, formas de autenticação e de manter integridade.

Um país que necessita se comunicar e escolhe limitar *sites*, a exemplo da China, consegue que determinadas empresas não tenham acessos massivos em seu país, não que nenhum cidadão tenha acesso. Uma análise dos sites mais visitados por pais[2], mostra que os sites das maiores empresas norte-americanas de tecnologia não são líderes em acesso somente em China e Rússia, que desde bastante tempo limitam a atuação de empresas estrangeiras nos países. Especialmente a China que conta com mais de 500 milhões de pessoas ativas que acessam a internet, há massa crítica e capital para investir em empresas que criaram soluções elegantes. Tais comentários são relevantes para ressaltar que tais medidas podem ser válidas em um contexto que o Estado priorize questões internas.

Outra questão relevante refere-se à possibilidade de exigir que uma informação armazenada em jurisdição alienígena, da qual a lei geral de proteção a dados traz diretrizes (Lei 13.709/2018, art. 3º). Deve-se notar que no ambiente digital o armazenamento pode facilmente ser feito em servidores em outros países, e é limitado pela largura de banda de transmissão e tempo de latência, algo que é consideravelmente reduzido com uso de fibras óticas e roteadores fotônicos (não elétricos). Se tais limites são reduzidos, soluções com redundância ou virtualização viram

[2] Vide sites de ranking de alcance, audiência e tempos gasto por usuários como https://www.alexa.com/topsites

a regra. A virtualização é a simulação de um ambiente de processamento dentro de outro, e também permite a serialização de estados completos (ou seja, transmissão em rede) e a criação de conjunto de dados que representam o instantâneo de todo um sistema ("snapshot"). Tais possibilidades também indicam a inutilidade jurídica da discussão de limitação a acesso de dados em função de onde estão armazenados. Trata-se de uma questão que é transferida do simples armazenamento para a possibilidade do processamento/tratamento de dados da maneira desejada, incluindo a capacidade técnica para tanto. Nesse sentido, o direito pode exigir a disponibilidade dos dados e seu tratamento adequado, algo mais parecido com o resultado, do que se imiscuir no como é feito, pois isso acaba recaindo em exercício de arbitrariedade ou ineficiência.

Deve-se mencionar que a coleta de dados sobre o usuário em geral é feita de forma gradual ou a partir de pequenas identificações. Assim, por exemplo, a pessoa pode fazer a autenticação com usuário e senha ou alguma biometria e na navegação online aquilo é simplificado para um "cookie", que pode ter sido armazenado anteriormente no dispositivo. Ademais, em qualquer comunicação pelo protocolo IP são enviados metadados que servem para identificar e permitir a conexão. O que é a pessoa/usuário e qual a probabilidade de certeza de que a conexão não foi usurpada, replicada, violada dependem desses dados e das sequencias de transações. Pode-se imaginar uma situação em que a pessoa viajou para o exterior, fez autenticação fora do país e criou uma chave de criptografia local, cuja chave simétrica está em servidor de outra empresa em jurisdição diversa. Essa aplicação foi baixada numa loja de aplicativos, se vale de um sistema de anúncios, pagamento e entregas terceirizado e reconhece a identidade por meio do *login* em uma rede social, que se vale de um serviço de e-mail e contatos de outra grande empresa. Esta é executada em um serviço em nuvem que indica no qual os dados podem estar em cerca de meia dúzia de locais no globo, com as devidas redundâncias. Um exemplo desses, que pode ser real, demonstra que os dados só são inteligíveis em conjunto e são criados e armazenados em locais e momentos distintos. Assim, mesmo numa situação usual e sem interesse em burlas, um pedido para baixar todos dados coletados no país de forma inteligível não é viável se não houver tal orientação *a priori*.

Tal cenário comprova que a simples procedência dos dados não é fator para garantir a sua recuperação em formas agregadas ou inteligíveis e, simplesmente mencionar que há barreira porque os dados estão no exterior é se valer de um argumento que ignora a estrutura de funcionamento da rede. Ademais, falar em dados pessoais e coletas pode abarcar algumas questões de privacidade, mas não abarca todo o entrelaçamento e nem dá subsídios para algo

mais específico ou complexo no sentido de investigação forense em tecnologia (ECKERT, 1992), em que níveis de certeza adequados sobre autoria, integridade são necessários. Também é essencial notar que a partir do momento em que muitos dados privados passaram a estar nas nuvens, associações menos formais que uma conta bancária ou cartão de crédito tornam-se relevantes. Em princípio, o simples fato de um perfil na rede social indicar o nome de alguém não fecha a questão sobre ser a pessoa, mas os constantes reforços e inserções de dados ligados a pessoa, suas atividades e amigos/contatos, tem o condão de tornar aquela identidade um ponto de confiabilidade, e algo relevante para uma pesquisa até criminal. Todavia, muito dessas informações dependem de heurísticas e associações, não sendo dados primários[3] (mas derivados) e muito do valor das associações dependem de mais estudos e análises[4].

Por essas considerações, no mínimo pode-se dizer que há dúvida fundada se a empresa responsável é acionada para responder dados a autoridade que não são informações primárias têm o dever legal de entregar informações como se fosse uma relatório gerencial, e na forma que o agente estatal gostaria de obter.

Neste contexto, a interferências estatais devem levar em consideração idiossincrasias e elementos de outros sistemas que não o jurídico. No sentido de Luhmann, um operador deve se valer dos canais e linguagem próprios, não de uma relação de poder que se impõe pela força (BAETA NEVES, MONTEIRO NEVES, 2006, p. 187). Nesse sentido, autoridades fiscais, antitruste, regulatórias, administrativas em geral, legislativas e judiciárias (cível e penal) e devem ter algum tipo de reconhecimento de limites e coordenação para incentivar ou propiciar comportamento de interesse público/específico e disruptivos. Também se deve mencionar que os incentivos não são estatais, mas podem ser sociais especialmente no sentido de reconhecimento ou conhecimento, incluindo propaganda e sentimentos. Indica-se que o uso de soluções *ad hoc* ou políticas públicas implementadas pelo Poder Judiciário podem não ser boa solução. O fato de existirem mecanismos para sigilo e integridade, dentre muitos outros, só

[3] Menciona-se dados primário no sentido da lei de acesso a informação ou de outros referências arquivísticas (Lei 12.527/2011):

Art. 4º Para os efeitos desta Lei, considera-se: (…) IX - primariedade: qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações.

[4] Vide o caso do vazamento de dados da "Cambridge Analytics" nas eleições americanas e no referendo do Brexit. Várias formas de associação são indicadas no documentário da Netflix "The great hack". Informações podem ser obtidas em <https://www.dn.pt/cultura/interior/the-great-hack-o-documentario-que-vai-mostrar-lhe-o-poder-dos-dados-que-oferece-as-empresas-11139410.html>, acesso em 23/12/2019.

reforça a questão que a exequibilidade de uma decisão, assim como seus efeitos e impactos, devem ser mensurados.

A questão de utilizar elementos da própria tecnologia ocorre por exemplo das decisões do STJ referentes ao direito ao esquecimento[5] em que se reconheceu a possibilidade do pedido, mesmo com fundamento em direito de imagem e atualidade, e se decidiu que é ônus do requerente indicar as URL[6], ao invés de formas de se identificar o conteúdo. Certamente, o fato de ser um direito pleiteado judicialmente encontra limites subjetivos da lide, o que justifica a indicação de sites. Todavia, o endereço do site não se confunde com o seu conteúdo, e, uma solução com maior efetividade seria o de prefixar indenização para reprodução do conteúdo, e verificar se é o conteúdo porque qualquer meio de prova por similaridade. São questões para as quais existem meios técnicos que poderiam ser referenciados na decisão, o que ampliaria seu alcance e efetividade.

Nesse sentido, o cenário estatal envolve oportunidades como também desafios. Entre as oportunidades, pode-se indicar o uso de algoritmos e massas de dados para detectar ou prevenir fraudes e crimes. Menciona-se que além da quantidade e de novas técnicas, há o fato de que mais dados privados são disponíveis para mineração e *big data*. Em relação a big data, indica-se que se relaciona à ciência, técnicas e metodologias que permitem uma análise em diversas dimensões de conjuntos de dados antes tidos como intratáveis[7]. A ampliação do horizonte daquilo que se considera tratável ou razoável, tem o condão de levantar questões jurídicas e preocupações. Indica-se também que a forma com que estados ou sociedades direcionam seus olhares para essas questões não é uniforme, e na sequência mostra-se que existem modelos diversos de tratamento de dados, o que ressalta a importância de que o Brasil não apenas copie ou importe um desses modelos.

---

[5] REsp 1334097/RJ, Rel. Ministro LUIS FELIPE SALOMÃO, QUARTA TURMA, julgado em 28/05/2013, DJe 10/09/2013; REsp 1335153/RJ, Rel. Ministro LUIS FELIPE SALOMÃO, QUARTA TURMA, julgado em 28/05/2013, DJe 10/09/2013;

[6] URL = universal resource locator, que é o endereço do site.

[7] "(1) Big Data is commonly understood as the use of large scale computing power and technologically advanced software in order to collect, process and analyse data characterised by a large volume, velocity, variety and value. These interdependent characteristics drive both the benefits and potential risks of Big Data from a competition policy perspective." (OCDE, 2016).

3 TRÊS MODELOS PARA TRATAMENTO DE DADOS: AMERICANO, EUROPEU, CHINÊS.

Um outro motivo que impõe dificuldades para atuação do Estado nacional é o fato de que modelos diferentes de formas de tratamento de dados coexistem no mundo. No artigo indica-se de uma maneira não exaustiva alguns pontos que diferenciam o modelo norte-americano, europeu e chinês em relação ao tratamento de dados digitais, a opção brasileira, que se assemelha ao último. Não se pretende fazer uma análise teórica exaustiva até porque se parte de constatações de fato e de situações que podem a vir sofrer alterações, justamente porque dependentes de um contexto político, jurídico, econômico e jurídico, mas se indicam pontos relevantes de cada modelo.

O modelo norte-americano se associa com a criação e expansão da Internet, em que foram pioneiros, com alguns aspectos como ausência da tarifas de interconexão e entre países e concentradores de tráfegos (“backbones”), controle relativamente técnico de questões de padrões e conexão (comitê de IETF), controle de elementos centrais pelo governo norte-americano ou entidades daquele país (ICANN e nomes, por exemplo), relativa pouco preocupação com tratamento de dados por privados e conceitos não legais como neutralidade de rede.

Em termos de dados, o direito à privacidade tem como histórico o conceito individual de privacidade (BRANDEIS; WARREN, 1890), e um viés mais coletivo surge somente mais tarde, especificamente em relação aos dados coletados por agências federais, que possuíam amplo acesso a dados de pessoas/cidadãos. Nesse sentido, pode-se mencionar O *Privacy Act* de 1974 que regulava o armazenamento de informações com dados pessoais, coleta, uso, manutenção e disseminação de dados entre agências federais. Apenas recentemente houve manifestação no sentido de se voltaram para equalizar posições com diretrizes europeias, deixando de lado a autorregulação das empresas e prevendo certas balizas mínimas no "*Consumer Privacy Bill of Rights"* de 2015 (VOSS; CASTETS-RENARD, 2016, p. 377)[8].

[8] A lei Americana seria uma resposta ao GDPR, regulamento geral de proteção de dados europeu e tem como fundamentos o controle individual sobre a coleta e uso, a transparência sobre privacidade e práticas de segurança, respeito ao contexto que justificou a coleta no sentido de um uso razoável, possibilidade de correção de dados incorretos, coleta de dados focada nos usos previstos e “accountability” no sentido de que deve ser verificável que as companhias estão aderentes aos princípios legais.

Tal modelo é o responsável, por exemplo, por serviços gratuitos remunerados por publicidade, facilidade em permitir investimento de *venture capital* e redução de custos iniciais, assim como pelo grande domínio entre termos de software e padrões, como também permitiu que algumas de suas empresas passassem a ter alcance e influência globais, com crescente preocupações sobre oligopólios e restrição à concorrência. Dentre as empresas, destaque para as 5 grandes "Big Tech" que são Apple, Amazon, Alphbet (Google), Microsoft e Facebook, que reúnem cerca de 15% do valor de mercado das bolsas americanas e são responsáveis por revoluções sociais apoiadas na tecnologia em muitos países (LEKKAS, 2019).

Já no modelo chinês, há controle estatal sobre conteúdos que podem ou não ser disponibilizados pelo site e grande liberdade para coleta e tratamento de dados digitais como reconhecimento facial e ainda, virtualmente ausência de barreiras para que empresas autorizadas a atuarem no país forneçam serviços integrados, inclusive aqueles que no ocidente são tradicionalmente regulados como serviços bancários ou consultas médicas realizadas a distância. O modelo asiático pauta-se pela concentração de indústrias de equipamentos (hardware), destaque para o pólo inovador de Shenzen, possibilidade de controlar ou manipular o câmbio e grande presença na infraestrutura de rede. Há grande destaque na mídia pela disputa entre EUA e China pela venda e controle do padrão das redes de telefonia 5G, com sanções à empresa chinesa com participação estatal Huawei. Deve-se ponderar que o modelo chinês traz vantagens óbvias como as de permitir que empresas gerem concorrência com empresas tradicionais e muitos campos (ZMOGINSKI, 2018)[9], o que aumenta a oferta de serviços, inclusive para a população de baixa renda, algo que o corporativismo tem afastado no âmbito nacional.

O modelo europeu pauta-se por uma preocupação grande com a privacidade e controle dos dados pelos usuários. Há algumas inovações que são pautadas pelo amplo mercado Europeu (cerca de 500 milhões de consumidores com renda elevada). Destacam-se elementos com a regulação do direito ao esquecimento, em que o *leading case* no ambiente digital é decisão contra o buscador Google na Espanha em 2011[10], em que se definiu a obrigação de não indexar

[9] O poder estatal chinês não impões barreiras a integração vertical em vários setores e empresas como Alibaba, Tencent e Baidu possuem sites de buscas, redes sociais como também serviços de pagamentos e bancos e seus aplicativos integram serviços e utilidades em nível mais amplo que seus congêneres ocidentais. Nesse contexto, o pagamento por celular já supera em valores o pagamento por cartão de crédito na China.

[10] Google Spain v. AEPD é uma decisão do Tribunal de Justiça da União Europeia que reconheceu o direito de ser esquecido sob a Diretiva de Proteção de Dados. Em 2010, Mario Costeja Gonzilez, cidadão espanhol, apresentou uma queixa ao espanhol Agência de Proteção de Dados ("Agência Espanhola de Proteção de Dados", "AEPD")

informações, mesmo que verdadeiras e mitigou o direito à informação. Também é relevante que se mencione a nova lei geral de proteção a dados europeia (regulação geral de proteção de dados) (REGULATION (EU) 2016/679), já em vigor, que traz diversos inovações e implica na existência de um escritório europeu de proteção a dados digitais, e que também é inspiração a lei nacional de proteção a dados (Lei nº 13.853/2019).

Deve-se considerar, todavia, que o regulamento em si pode levar a excesso de regulação e pode levar a efeitos indesejados com perda da capacidade de inovação e dificuldade em lidar com vários aspectos que são considerados vantagens do modelo de rede aberta (COUNCIL, 2018)[11]. A regulação em si pode agir como uma barreira de mercado. A recente decisão alemã de exigir requisitos não funcionais os fornecedores de equipamentos de redes de telefonia 5G é basicamente uma forma indireta de bloquear empresas chinesas.

Ademais, uma vantagem do que modelo europeu são os recentes avanços em relação às proposições de novas formas de taxação de transações online, ou de formas de compartilhamento de receita em sites noticiosos e de imagens.

A existência de interesses e critérios diversos na forma de normatizar e regular setores indica que podem existir dificuldades na cooperação e troca de informações internacionais. Ademais, o próprio conceito do que se entende por excessiva concentração de mercado assume feições diferenciadas, especialmente quando se verifica a forma de atuação das 5 grandes empresas de tecnologia norte-americanas, que têm alcance global mas atuam em nichos, em das empresas chinesas, em que se admitem diversas formas de verticalização.

contra a La Vanguardia Ediciones SL, uma grande editora de notícias diárias na Espanha, além do Google Espanha e Google Inc. "

[11] O site da Forbes indica ao menos 15 efeitos colaterais indesejados e não planejados da GDPR tais como: 1. Restrição de privacidade e inovação 2. Obstáculos para armazenamento de dados Blockchain 3. Desgaste de Opt-In 4. Baixa qualidade do atendimento ao cliente 5. Comprometimento dos pequenos negócios 6. A morte lenta dos serviços gratuitos 7. Regulamentação semelhante nos Estados Unidos 8. A fotografia como parte do GDPR 9. C-Suite assumindo a responsabilidade pela segurança de dados 10. Acesso restrito aos cidadãos da União Europeia 11. Capacidade reduzida de rastreio do cibercrime 12. Maior envolvimento do cliente 13. Legislação do país em desacordo com o GDPR 14. Sites norte-americanos negam acesso a visitantes da União Europeia 15. Valor agregado aos dados primários.

4 CONTEXTO NACIONAL: MARCO CIVIL E LEI DE PROTEÇÃO A DADOS

O cenário nacional indica que o país tem importado parte substancial do modelo europeu de tratamento de dados, especialmente com a aprovação da Lei nº 13.853, de 8 de julho de 2019 e a criação da "Autoridade Nacional de Proteção de Dados". Todavia, de plano se verifica que não foram feitos maiores estudos sobre os impactos negativos das propostas europeias, que não podem ser negligenciados. Por exemplo, no âmbito da tributação ainda se discute a volta de alguma CPMF ou contribuição sobre transações digitais, ao invés de se buscar o entendimento sobre os efetivos problemas das transações digitais.

Também se menciona que o país já criou exceções legais ao regime de tratamento de dados da lei de proteção, como é o caso da lei do cadastro positivo (alterações da LC nº 166/2019). No mesmo sentido, menciona-se o regulamento do cadastro base do cidadão, pelo governo federal, que não endereça quaisquer das preocupações da lei de proteção à dados. Nesse sentido e em resumo, há falta de uniformidade no tratamento dos dados e exceções legais que possivelmente permitirão que tais situações sejam a regra, não a exceção.

Ademais, no caso do Brasil, menciona-se que a CF/88 teve seu artigo 171 revogado (EC 6/1995) e juridicamente não é compatível a solução chinesa dentro do ordenamento nacional de maneira simplista, mas isso não significa que o estado não deve regular a atividade digital, pelo contrário. De um lado implicam em que os juristas reconheçam limitações ou o *modus operandi* dos sistemas digitais e não lhe retirem meios para que o ambiente mantenha a possibilidade disruptiva. Também significa que há mais atores e valores que devem ser atendidos em eventual regulação, o que ressalta o tamanho do desafio estatal em regular bem e adequadamente. Indica também que a regulação deve envolver aspectos de coordenação entre exploração da atividade econômica, inovação, preservação da concorrência, questões criminais, interesses particulares que também são direitos fundamentais. Nesse ponto, destaca-se que a regulação vem avançando, transformando-se em algo em que o **interesse público e privado não são necessariamente excludentes**. Segundo Marco Antônio Pinto Florêncio Filho e Amanda Scalise Silva (2019, p. 239) a regulação de cunho econômica passa por 3 fases, quais sejam, i) regulação privada, focada no indivíduo, ii) regulação pública fundada na crença de que o Estado pode ser indutor de crescimento e iii) corregulação público-privada, em que a regulação impõe certos deveres públicos às empresas, que fogem de riscos, e uma certa abstenção estatal.

Deve-se considerar, todavia, que a regulação em sentido amplo requer a uniformização e a atualização do feixe normativo que se aplica às operações, empresas e usuários na internet. Tal

descompasso pode ser evidenciado em diplomas como o Marco Civil da Internet e a Lei geral de telecomunicações.

No caso do Marco civil da Internet (Lei nº 12.965/2014), há uma divisão entre provedores de conexão e de conteúdo (artigos 11 e 15), em que basicamente no segundo não há responsabilização, ao contrário do primeiro. Já a Lei Geral de Telecomunicações (LGT, Lei nº 9472/1997), que regulamenta um tema de atividade legislativa privativa da União (CF/88, art. 22, "IV") estabeleceu direitos e deveres que se mostram anacrônicos como o decréscimo da telefonia fixa em cabos de cobre e diminuição de ligações de voz por celulares. Há a categoria de serviços de valor adicionado (art. 61 da LGT[12]) que de um lado aparenta ser algo fora do escopo legislativo da União e de outro representa uma brecha para que empresas de telefonia prestem serviços diversos, mas também se confunde com "acesso condicionado" ou TV paga. Por exemplo, na ADI 6269/RO rechaçou-se lei estadual que veda a oferta de serviços de valor adicionado por empresa de telefonia, por incompetência formal. De outro lado, houve recente decisão que permitiu à Fox a oferta de seus canais via *streaming* (internet) uma vez que a lei não teria previsto tal hipótese, e aplicar-se-ia a liberdade de iniciativa (GOMES, 2019)[13].

Nesse sentido, verifica-se que o feixe normativo que se aplica a telecomunicações, internet, empresas de TV a cabo é dispare e não se coaduna com a convergência tecnológica. Nesse sentido, também se indica a Ação direta de Constitucionalidade (ADC) 51[14], na qual é questionada a natureza jurídica dos provedores de aplicações e serviços e especificamente se devem ser regulados como telecomunicação ou se sujeitar a leis de outro temática.

A questão é mais complexa e não se restringe a dificuldade nacionais. As chamadas aplicações *Over the Top* (OOT) são aquelas que se valem de camadas da Internet e se utilizam da comunicação como um bem público ou de interesse especial em que o acesso não deveria ser restringido ou feito com barreiras técnicas, jurídicas ou comerciais que privilegiem alguns em detrimento de outros. Mesmo questões como universalidade da rede não são tão simples, uma

[12] Art. 61. Serviço de valor adicionado é a atividade que acrescenta, a um serviço de telecomunicações que lhe dá suporte e com o qual não se confunde, novas utilidades relacionadas ao acesso, armazenamento, apresentação, movimentação ou recuperação de informações.

[13] Argumentou-se que na edição da lei da TV por assinatura 12.485/2011, a realidade do mercado era completamente distinta da atual e não se aplicaria ao contexto vigente. Como exemplo, indicou-se que Não havia serviços de 'streaming', e tampouco aplicativos com transmissão simultânea de conteúdos.

[14] Aa ação foi proposta pelo Instituto de Referência em Internet e Sociedade – IRIS, Petição Inicial ADC STF 51, em 27/03/2018.

vez que grandes provedores de conteúdo podem pagar para ter acesso a roteadores específicos, garantindo uma certa qualidade na transmissão. Não seria a oferta de um serviço pior para os demais, mas uma estratégia que permite melhor oferta, mas que de certa forma pode restringir a entrada de concorrente e inovação.

Já a discussão da ADC 51 e dos serviços OOT são relevantes para temas como competitividade, mas também para se determinar quais são as obrigações perante a uma requisição judicial, inclusive a empresa sediada no exterior ou com dados armazenados em outras jurisdições. Deve-se mencionar que por mais que os usuários finais tenham direito e previsão legal a terem acesso a seus dados, isso é irrelevante para os dados analíticos e gerenciais que são demandados por autoridades judiciárias ou administrativas para cumprirem determinados fins. Talvez seja o momento de o legislador nacional e os regulares se coordenarem e se valerem das oportunidades que as comunicações digitais propiciam, não suas limitações.

Também se mostra inviável que a uma determinada empresa se imponham restrições ou exigências sem contrapartida nas demais, sob pena de viola a isonomia, neutralidade. É algo que sai da esfera judicial usual, ou que demandaria decisão que para muitos transborda o papel do Poder Judiciário. Por outro lado, a irresponsabilidade das empresas não encontra respaldo em princípios constitucionais e mesmo em leis que estabelecem regras de *compliance* a exemplo da Lei nº 12.846/2013 e outros direitos fundamentais. Nesse sentido, apesar de não afastar de forma peremptória eventual punição à empresa, a conformidade com boas práticas se mostra útil a afastar dolo de dever de cuidado *(*SAAD-DINIZ; ADACHI; DOMINGUES, 2016, p. 97).

Em se tratando de persecução penal, há que se mencionar que a isonomia envolve a paridade de armas e previsibilidade na obtenção de dados, de modo a assegurar uma persecução penal equânime (GROSSI, 2014, p. 14). Tais considerações são relevantes mesmo porque os dados de aplicativos de internet são contextuais e, para ampla defesa, é necessário que se indique os elementos que permitem verificar a acuracidade, integridade e relação com autoria dos dados. Esses elementos, como se mostrou no artigo, não são triviais e tampouco são representados por dados/informações individualizadas. Nesse sentido, faz necessário que se especifiquem elementos que permitam até mesmo a previsibilidade para o acusado. Como mencionado, o Marco civil é lacônico no que se refere a obrigações de provedores de conteúdo.

Também deve ficar mais claro qual papel desejado para o desenvolvimento de setores críticos tendo em vista o desenvolvimento nacional. Deve-se mencionar que o Brasil não conta com o

pioneirismo americano, com o tamanho e uniformidade do mercado europeu e nem pode implantar mecanismos de controle com os feitos na China. Todavia, não significa que deva abdicar de regular, normatizar e buscar um melhor equilíbrio entre interesses público e privados.

Por exemplo, há aspectos de outros modelos que poderiam ser considerados no país, a exemplo da permissividade chinesa para reconhecimento facial ao menos em termos de segurança. É bem verdade que o Brasil tem usado de reconhecimento facial em aeroportos e fronteiras terrestre, mas não o faz com regulamentação legal (apenas portarias) e de uma forma sistêmica em termos de algoritmos e transparência, por exemplo, evitando vícios estatísticos ou pré-condicionamento nos graus de acuracidade exigidos (O'NEIL, 2019).

Com a COVID-19, a busca de soluções de integração de dados e a preocupação com a privacidade mostram-se um problema imediato e de escala global. Isso incluiu oportunidades para diversas empresas de tecnologia proporem formas de automatizar diagnósticos ou avaliar graus de isolamento (DROZDIAK; ACKERMAN; LINDBERG, SOO, 2020). Ademais, a pandemia mostrou que estratégias nacionais diferentes obtiveram resultados díspares, sendo a eventual gravidade e aprofundamento pode ser até mesmo um fator para desestabilização democrática.

5 CONCLUSÕES

A obtenção de dados sobre usos de aplicativos digitais não é direto ou natural e sua obtenção pelo Estado conforme o direito, requer planejamento e coordenação normativa, regulatória e administrativa. A complexidades inerente a um sistema diverso do jurídico tem que ser refletida nas normas e representam desafios para o Estado nacional em termos de tecnologia, poder e dimensão das empresas, assim como interesses diversos e mesmo antagônicos de outros Estados. No artigo indicam-se elementos do modelo de tratamento de dados e acesso ao bem público Internet dos EUA, Europa e China, indicando preocupações e vantagens de cada abordagem, e como se relaciona com normas do contexto nacional.

Indica-se que a solução não deve se limitar a copiar um modelo, mas ponderar adequadamente elementos e interesses, buscando criar um ambiente que proteja interesses individuais, mas permita inovações, e principalmente, reduzir distorções históricas da sociedade brasileira. Nesse sentido, há que se repensar o papel dos provedores de aplicação (Marco Civil) e evitar os excessos da regulação de proteção a dados.

6 REFERÊNCIAS

BAETA NEVES, Clarissa Eckert; MONTEIRO NEVES, Fabrício. *O que há de complexo no mundo complexo? Niklas Luhmann e a Teoria dos Sistemas Sociais*. In Sociologias, Porto Alegre, ano 8, nº 15, jan/jun 2006, p. 182-207.

BRANDEIS, Louis; WARREN, Samuel. "*The Right to Privacy*". In Harvard Law Review. Vol. IV December 15, nº 5, 1890. Disponível em http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html , acesso em 20/08/2016.

COUNCIL, Forbes Technology. *15 consequências inesperadas do GDPR*. Em 28/08/2018. Disponível em https://forbes.com.br/negocios/2018/08/15-consequencias-inesperadas-do-gdpr/ , acesso em 26/12/2019.

ECKERT, William G. *Introduction to forensic sciences*. Second editon/ William G. Eckert. Originally published: New York: Elsevier, 1992.

FILHO, Marco Antônio Pinto Florêncio; SILVA, Amanda Scalise, *A repercussão da governança na responsabilidade Penal da Pessoa Física e Jurídica*. In Compliance e Direiot Penal econômico / Fábio Ramazzini Bechara. São Paulo: Almedia, 2019.

GOMES. Helton Simões. *Justiça libera Fox para oferecer canais de TV paga via streaming*. In Tilt,São Paulo, 18/12/2019. Disponível em https://www.uol.com.br/tilt/noticias/redacao/2019/12/18/justica-libera-fox-para-oferecer-canais-de-tv-paga-via-streaming.htm , acesso em 27/12/2019.

DROZDIAK, Natalia; ACKERMAN, Gwen; LINDBERG; SOO, Kari. The Virus Gives AI a Chance to Prove It Can Be a Force for Good. In Bloomberg Bussinessweek, em 7 de abril de 2020. Disponível em https://www.bloomberg.com/news/articles/2020-04-07/coronavirus-giving-ai-a-chance-to-prove-it-can-be-force-for-good, acesso em 08/04/2020.

GROSSI, Viviane Ceolin Dallasta Del. A defesa na cooperação jurídica internacional penal. Viviane Ceolin Dallasta Del Grossi. -- São Paulo: USP / Faculdade de Direito, 2014.

LEKKAS, Nicolas, *The Big Five Tech Companies & Their Big Five Acquisitions*. In CULTURE, INFOGRAPHIC, APRIL 2019. Disponível em https://growthrocks.com/blog/big-five-tech-companies-acquisitions/, acesso em 26/12/2019.

LUHMANN, Niklas. *O direito da sociedade*. São Paulo: Martins Fontes, 2016.

OCDE, the Secretariat. *Big Data: Bringing Competition Policy to the Digital Era*. Executive Summary. 29-30 november 2016. Disponível em <www.oecd.org/daf/competition/big-data-bringing-competition-policy-to-the-digital-era.htm>

OECD, *Algorithms and Collusion: Competition Policy in the Digital Age*. Publicado em 2017, disponível em http://www.oecd.org/competition/algorithms-collusion-competition-policy-in-the-digital-age.htm, acesso em 27/12/2019.

O'NEIL, Cathy. *Amazon Can't Fix Facial Recognition. In Technology & Ideas*. Bloomberg Opinion, em 24/01/2019. Disponível em https://www.bloomberg.com/opinion/articles/2019-01-24/amazon-can-t-fix-facial-recognition, acesso em 29/12/2019.

RICHARDS, Neil M.; KING, Jonathan H.. *Big data ethic*s. In 49 Wake Forest L. Rev. 393, 2014.

SAAD-DINIZ, Eduardo; ADACHI, Pedro Podboi; DOMINGUES, Juliana Oliveira (Org.). *Tendências em governança corporativa e compliance*. São Paulo: LiberArts, 2016.

TANENBAUM, Andrew S.. *Computer Networks*, 4th Edition, (Prentice-Hall, 2002).

VOSS, W. Gregory; CASTETS-RENARD, Céline. *Proposal For An International Taxonomy on the Various Forms Of The "right To Be Forgotten": A Study On The Convergence Of Norms*. In Journal on Telecomm. & High Tech. L. 281, 2015-2016, p. 310-311.

ZMOGINSKI, Felipe. *Mobile payment superará gastos com cartão de crédito na China em 2018*. UOL, canal Tilt em 05/05/2018. Disponível em https://copyfromchina.blogosfera.uol.com.br/2018/05/02/a-china-esta-pronta-para-dizer-tchau-para-dinheiro-e-cartoes-de-credito/, acesso em 26/12/2019.