FACULDADE DE DIREITO – FD

CLÁUDIA ADRIANA L. V. TOLEDO

Da Violação de Dados Pessoais e o Direito à Privacidade

Brasília

2018

Cláudia Adriana L. V. Toledo

DA VIOLAÇÃO DE DADOS PESSOAIS E O DIREITO À PRIVACIDADE

Monografia apresentada à Faculdade de Direito da Universidade de Brasília como requisito parcial para obtenção da graduação em Direito

Área de Concentração: Direito Civil, Direito Internacional Público, Direito Digital.

Orientador: Prof. Dr. Alexandre Kehrig Veronese

Brasília – Distrito Federal

2018

Toledo, Cláudia Adriana L. V.
Da violação de dados pessoais e o direito à privacidade/
Cláudia Adriana L. V. Toledo; orientador: Alexandre Kehrig Veronese. -- Brasília, 2018.
64 p.
Monografia (Graduação - Direito) – Universidade de Brasília, Brasília, 2018.
1. Evolução Histórica. 2. Violação de dados. 3. RGPD. 4. Legislação Brasileira. 5. Convergência. I. Veronese, Alexandre Kehrig, orient. II. Título.

CLÁUDIA ADRIANA L. V. TOLEDO

DA VIOLAÇÃO DE DADOS PESSOAIS E O DIREITO À PRIVACIDADE

Trabalho de conclusão de curso apresentado à disciplina Redação de Monografia (FDD), do Curso de Graduação em Direito, na Faculdade de Direito na Universidade de Brasília, como requisito parcial à obtenção do título de Bacharel em Direito.

BANCA EXAMINADORA

_____

Orientador: Prof. Doutor Alexandre Kehrig Veronese – Orientador

FD/UnB

_____

Membro: Prof. Mestre Frank Ned Santa Cruz de Oliveira – Examinador

FD/UnB

_____

Membro: Prof. Doutor Wilson Roberto Theodoro Filho

FD/UnB

_____

Suplente: Prof. Doutor Mamede Said Maia Filho

FD/UnB

Brasília, _____ de _____ de 2018

Aos meus familiares pelo apoio oferecido nos momentos de felicidade, como também de incerteza. Obrigada pela força!
À todos que se interessam e lutam pela manutenção e respeito à privacidade do que nos é mais caro: nós mesmos!

"...**toda pessoa é única e nela já habita o todo universal**, o que faz dela um todo inserido no todo da existência humana; que por isso ela deve ser vista antes como centelha que condiciona a chama e a mantém viva, e na chama a todo instante crepita, renovando-se criadoramente, sem reduzir uma à outra; e que, afinal, embora precária a imagem, o que importa é tornar claro que dizer pessoa é dizer *singularidade*, *intencionalidade*, *liberdade*, *inovação*, e *transcendência*, o que é impossível em qualquer concepção personalista a cuja luz a pessoa perde os seus atributos como valor-fonte da experiência ética para ser vista como simples "momento de um ser transpessoal" ou peça de um gigantesco mecanismo, que, sob várias denominações **pode ocultar sempre o mesmo "monstro frio"**: "coletividade", "espécie", "nação", "classe", "raça", "ideia", "espírito universal" ou "**consciência coletiva**" " (REALE, Miguel, 1963, apud COELHO, Inocêncio Mártires, 2009, p.172) – *grifo nosso*.

RESUMO

O presente estudo tem o condão de expor a evolução legal da privacidade atrelada aos dados pessoais, algumas violações a esses dados e os prejuízos decorrentes de sua exposição em detrimento ao direito à privacidade e intimidade, primordial ao desenvolvimento psíquico e emocional humano. Em vista disso, há a preocupação em elaborar legislações específicas, que tratem sobre o tema da defesa das informações pessoais, amplas o suficiente a fim de que haja convergência do ordenamento jurídico correspondente entre diversos países. A coadunação entre normas facilita o livre fluxo dos dados e, consequentemente, propicia o crescimento da economia digital. Assim, para que ocorra a convergência entre ordenamentos jurídicos distintos é mister que haja intersecção entre elas em determinados aspectos. Alguns deles referem-se ao consentimento dado pelo usuário quanto à utilização de seus dados, o acesso à informação sobre o compartilhamento desses dados com terceiros e como são utilizados, a presença de uma Autoridade Nacional de Proteção de Dados a quem o usuário possa se reportar, a cominação de sanções em caso desrespeito à privacidade e a exclusão dos dados quando houver solicitação. No entanto, o que está em jogo é o alcance da norma reguladora ao objetivo de promover a segurança dos dados e sua implementação diante de um mundo regido e constantemente alterado por tecnologias digitais no que diz respeito às constantes transformações das relações pessoais, econômicas, políticas e sociais.

Palavras-chave: Evolução Histórica. Violação de dados. RGPD. Legislação Brasileira. 5. Convergência.

ABSTRACT

The present study has the purpose of exposing the legal evolution of privacy related to personal data, some violations of this data and the damages resulting from its exposure in detriment to the right to privacy and intimacy, primordial to human psychic and emotional development. In view of this, there is a concern to elaborate specific legislation dealing with the subject of the protection of personal information, which is broad enough that there is convergence of the corresponding legal system between different countries. Coordination between standards facilitates the free flow of data and, consequently, promotes the growth of the digital economy. Thus, in order for convergence to take place between distinct legal systems, it is necessary that there be an intersection between them in certain aspects. Some of them refer to the consent given by the user regarding the use of their data, access to information on the sharing of this data with third parties and how they are used, the presence of a National Data Protection Authority to whom the user may report the payment of penalties in case of disrespect to privacy and the exclusion of data when requested. However, what is at stake is the scope of the regulatory norm to the goal of promoting data security and its implementation in the face of a world ruled and constantly altered by digital technologies with regard to the constant transformation of personal, economic, political, and social relations.

Keywords: Historic evolution. Data breach. RGPD. Brazilian legislation. 5. Convergence.

LISTA DE ABREVIATURAS E SIGLAS

ACP – Ação Civil Pública

API (IPA) - *Application Programming Interface* (Interface de Programação de Aplicativos)

Art. – Artigo

AWS – Amazon Web Services

BCE – Biblioteca Central da UnB

Brexit – *British exit*

CA – Cambridge Analytica

CDC – Código de Defesa do Consumidor

C.E. – Comunidade Europeia

CEDH – Convenção Europeia para proteção dos Direitos do Homem e das Liberdades Fundamentais

CEO – *Chief Executive Office*

CF – Constituição Federal

COPPA – *Children's Online Privacy Protection Act of 1998*

Coord. – Coordenador

DPC - *Irich Data Portection Comissioner*

EC – Emenda Constitucional

EPCA – *Electronic Communications Privacy Act of 1986*

Et al. – *Et alli*

FCO - *Federal Cartel Office*

FTC – *Federal Trade Comission*

FTP (PTA) - *File Transfer Protocol* (Protocolo de Transferência de Arquivos)

HDSG – *Hessisches Datenschutzgesetz*

ICO - *Watchdog Information Commissioner's Office*

Inc. – inciso

IP – *Internet Protocol*

LPDP – Lei de Proteção de Dados Pessoais

MPDFT – Ministério Público do Distrito Federal e Territórios

MPRJ – Ministério Público do Rio de Janeiro

N° - número

OCDE – Organização para a Cooperação e Desenvolvimento Econômico

OEA (OAS) – Organização dos Estados Americanos (*Organization American States*)

ONU – Organização das Nações Unidas

PL – Projeto de Lei

Rel. – Relator

RGPD (GDPR) – Regulamento Geral de Proteção de Dados Pessoais (General Data Protection Regulation)

Res. – Resolução

SENACON – Secretaria Nacional do Consumidor

STF – Supremo Tribunal Federal

STJ – Superior Tribunal de Justiça

U.E. – União Europeia

UnB – Universidade de Brasília

SUMÁRIO

INTRODUÇÃO

Ao conceber a Declaração de Independência do Ciberespaço[1], John Barlow delineava um mundo separado de governos burocráticos, nos quais as normas destes seriam cerceadoras da liberdade individual. Além disso, não seriam capazes de dar a independência própria dos indivíduos que têm na rede sua nação.

As transformações decorrentes do livre acesso à Internet dão a impressão de que o ciberespaço seria um planeta sem lei ou mesmo regido pelo seu próprio Contrato Social, cujo fundamento maior é a liberdade de expressão, à parte do ordenamento jurídico das nações, no qual tudo seria permitido com a garantia da aparente invisibilidade do usuário (e tudo seria resolvido por lá mesmo!).

Muitas vezes os códigos e legislações cíveis e penais não conseguem acompanhar a velocidade com que novas relações sociais – e novos crimes – surgem e são praticadas no ambiente virtual. Então, o direito que regulava a interação entre as pessoas e procurava manter a ordem social, considerado de vanguarda, inclusive, passou a ficar atrás das interações sociais geridas pela Internet. Simplesmente, o legislador não consegue antever todas as situações que necessitarão de intervenção jurídica, então edita normas de caráter geral.

A mobilização para a proteção de dados pessoais talvez não houvesse ocorrido se chefes de Governo e de Estado, além de pessoas altamente influentes, não fossem atingidos pela espionagem, promovida pela Agência Nacional Americana (NSA), cujas ações reveladas por Edward Snowden, infringiram o sigilo das comunicações. Acrescente-se a atuação de hackers e crackers em relação à "quebra" de sigilo de dados pessoais, manuseio indevido de informações pessoais sensíveis e sua divulgação ao público, como exposição de fotos íntimas de celebridades. Outro ponto relevante é a guerra comercial entre países na disputa por dados econômicos, financeiros, sociais e pessoais, pondo em risco relações diplomáticas. Essas foram algumas questões pontuais para que a produção legislativa se voltasse para a criação de norma específica para a segurança dos dados.

No que diz respeito à privacidade, as normas dos mundos virtual e físico encontram dificuldades em garantir segurança a seus cidadãos, em virtude da alta velocidade de tráfego de informações. E isso é cada vez mais evidente à proporção em que o elo entre o real e o

[1] Disponível em: <http://www.dhnet.org.br/ciber/textos/barlow.htm> Acesso em: 01 dez. 2018.

digital chega a quase inexistir em algumas situações, como, por exemplo, o desenvolvimento de relacionamentos amorosos com namoradas virtuais[2].

Hodiernamente, os dados pessoais representam o combustível da economia digital. Reconhecidos como ativos para empresas, sociedade, governos e indivíduos, são necessários para implementação de políticas públicas e movimentação do mercado financeiro de ações. O cadastro das informações pessoais feito por estabelecimentos comerciais e prestadores de serviços é instrumento de observação do comportamento dos consumidores e é objeto de negociações com parceiros comerciais. Nesse contexto, a vulnerabilidade do titular dos dados é patente.

O efeito da ausência de uma legislação específica sobre dados é a exposição de consumidores titulares a riscos, pois os controladores e processadores não contemplam a adoção de práticas adequadas à defesa dos dados[3].

Outro obstáculo enfrentado pelo titular dos dados é a burocracia quanto ao apagamento de conteúdo pessoal, conhecido como direito ao esquecimento, ínsito à privacidade. Mesmo após o encerramento do pedido de retirada dessas informações cadastrais dos bancos de dados de instituições públicas e privadas, não há certeza de sua real exclusão[4].

Nessa tessitura, o desenvolvimento histórico da legislação sobre privacidade de dados, conforme exposto no Capítulo 1 é de fundamental importância para se compreender o quão dileto é o direito à privacidade e intimidade no desenvolvimento da personalidade, sendo cada pessoa um ser único. Em dicotomia a esta secção, o Capítulo 2 trata de alguns casos de violação de dados pessoais e o quanto o desrespeito à privacidade das informações podem atingir desde a vida pessoal até as relações internacionais. Com o objetivo de dirimir as consequências negativas das violações e dispor sobre direitos dos usuários/consumidores a União Europeia instituiu o Regulamento Geral de Proteção de Dados Pessoais, sobre o qual o Capítulo 3 apresentará um breve escopo. Já o Capítulo 4 discorre brevemente acerca da produção legislativa brasileira que culminou na criação da Lei de Proteção de Dados Pessoais e apresenta alguns princípios do Diploma Consumerista coadunados com os fundamentos da norma protetiva dos dados. Por fim, o Capítulo 5 traz alguns pontos de convergência entre a novel legislação brasileira e o Regulamento Europeu.

---

[2] No Japão, a categoria de solteiros denominada *otakus* prefere o jogo virtual *LovePlus* a ter um relacionamento amoroso 'real'.

[3] Diariamente, violações dos bancos de dados de organizações ocorrem por fragilidade na segurança. O *Breach Level Index* demonstra, em números, relatórios diários sobre ocorrências e o *ranking* das empresas de maior risco. Vide Anexo 1.

[4] Em 2011 Max Shrems promoveu ação contra o Facebook por este manter guardados seus dados pessoais, inclusive os que já haviam sido apagados. Disponível em: <https://olhardigital.com.br/noticia/facebook-tera-de-pagar-r245-mil-por-guardar-dados-que-foram-deletados/22681> Acessado em: 12 nov. 2018.

CAPÍTULO 1 – BREVE EVOLUÇÃO HISTÓRICA SOBRE A PROTEÇÃO DE DADOS PESSOAIS

Os usuários têm informações coletadas pelos provedores de conteúdo sob o argumento de "melhorar a experiência", conforme os termos de uso e políticas de privacidade. A coleta, no entanto, é realizada para compartilhar dados pessoais com empresas parceiras de provedores de acesso, redes sociais, aplicativos, a fim de direcionar campanhas publicitárias conforme o perfil do usuário. Essa personalização de bens e serviços origina *profiling*, ou perfilamento, em tradução livre, obtido através do emprego de *softwares* que têm a função de executar o rastreamento profundo de dados e informações com os hábitos e gostos dos consumidores. A análise desses dados influencia na abordagem dos usuários e nos serviços ou produtos oferecidos: modalidades de empréstimo e encargos associados àqueles, contratação de diversos tipos de seguros, aplicações financeiras adequadas ao estilo do cliente, dentre outros.

Os dados coletados podem se referir a informações obtidas *on-line* e *off-line* e abrangem sentimentos, manifestações de apreço ou desafeto, localização geográfica, histórico de navegação, hábitos de compra ou venda, como também a intenção de consumir, manifesta em muitos *e-commerces* com um coração, atribuindo caráter emocional à operação. Dessa forma, o detalhamento das informações corrobora com uma classificação mais refinada dos usuários de modo que se possa atingir desde as expectativas do público em geral até ser possível chegar na escala de um para um. Vê-se o acelerado crescimento tecnológico e isso interfere nas relações humanas cada vez mais dinamizadas e diversificadas a ponto de as normas que as regulam, embora atuais, não acompanharem a celeridade das relações jurídicas otimizadas no espaço de comunicação da rede de computadores, ou ciberespaço[5]. A facilidade de acesso à informação, a praticidade nas relações de consumo com utilização de diversas

[5] A construção da comunicação ocorre sem a presença física de quem interage, "dando ênfase ao ato da imaginação, necessária para a criação de uma imagem anônima, que terá comunhão com os demais. É o espaço virtual para a comunicação que surge da interconexão das redes de dispositivos digitais interligados no planeta, incluindo seus documentos, programas e dados, portanto não se refere apenas à infraestrutura material da comunicação digital, mas também ao universo de informações que ela abriga. O conceito de ciberespaço, ao mesmo tempo, inclui os sujeitos e instituições que participam da interconectividade e o espaço que interliga pessoas, documentos e máquinas. O ciberespaço representa a capacidade dos indivíduos de se relacionar criando redes que estão cada vez mais conectadas a um número maior de pontos, tornando-se as fontes de informação mais acessíveis". Fonte: Wikipedia. Disponível em <https://pt.wikipedia.org/wiki/Ciberespa%C3%A7o>. Acesso em: 08 set. 2018.

formas de pagamento, sendo ainda a principal por cartão de crédito, o desenvolvimento das comunicações interpessoais trouxe (r)evolução social e porque não falar uma (r)evolução econômica, pois as pessoas têm a disponibilidade de *sites* e aplicativos para celular que lhes permitem conhecer um possível parceiro, realizar casamentos, fazer pagamento de contas, investir em ações e fechar negócios *on-line*, e até comandar eletrodomésticos ou a própria casa remotamente bastando, para isso, ter em mãos um aparelho com plataforma que comporte tais funcionalidades. Vê-se que a 'era digital' representou um grande salto na história e como assevera Luiz Carlos Neitzel[6]:

> "Constata-se que sempre há movimentos crescentes e sucessivos na história: da oralidade para a escrita, da escrita para a imprensa, desta para o rádio e para a televisão, até chegar-se à informática. O aperfeiçoamento dos meios de veicular a informação foram criados pela necessidade de o homem se comunicar. O ser humano, ao longo de sua história, mantém-se sempre na expectativa de desvelar novos horizontes, explorar territórios alheios, impulsionado pelo desejo de interação, de descoberta. A invenção da imprensa veio ao encontro desse desejo, "divide-se a História em antes e depois do surgimento da escrita".

Não obstante as comodidades proporcionadas com as tecnologias digitais que se superam cotidianamente, há o impasse entre a vida privada e o direito social ao acesso à informação, pois a depender da situação o sigilo é resguardado caso a segurança do Estado e da sociedade sejam ameaçadas[7]. Também se assegura a privacidade quando o conhecimento público pode levar a discriminações, perseguições e constrangimentos que prejudiquem aspectos da vida pessoal a fim de assegurar o direito à dignidade.

Como um sistema que se comunica com outros, o direito busca regular e harmonizar os meios econômicos, sociais e agora o digital. Dessa forma, quando trata dos diretos de acesso à informação deve-se assegurar, também, e de forma equânime, a proteção dos indivíduos, dispondo de meios que lhe assegurem a resposta aos abusos cometidos em nome do conhecimento público.

O Estado Democrático de Direito tem como princípios basilares a tutela da intimidade e o direito à informação, devendo, portanto, passar pelo equilíbrio/ponderação dos direitos fundamentais a fim de que não embaracem suas respectivas aplicações, com a garantia de que o fluxo de informações virtuais não sofra com o processo burocrático da criação de normas de

---

[6] LIMA, Rogerio Montai de. *Relações contratuais na Internet e Proteção Jurídica do Consumidor*. Dissertação de mestrado em Direito, UNIMAR: 2006. p. 17. Disponível em <http://www.geocities.com/Athens/Sparta/1350/evolucao_comunic.htm.> Acesso em: 08 set. 2018.

[7] BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal: Centro Gráfico, 1988. 292 p.

proteção de dados. Nesse diapasão uma relação jurídica deve ser estabelecida como fundamento de atribuição de uma obrigação de respeito à privacidade, e por conseguinte, a dados de pessoas físicas e jurídicas.

Como direitos atinentes à privacidade está "o direito de o indivíduo excluir do conhecimento de terceiros aquilo que só a ele é pertinente e que diz respeito ao seu modo de ser exclusivo no âmbito de sua vida privada[8]", que se aplica ao direito ao esquecimento ou apagamento com desprendimento dos fatos pretéritos à vida atual da pessoa por ter estes perdido o interesse social da informação, apesar de sua veracidade.

Amparada pelo artigo 12 da Declaração Universal dos Direitos do Homem, a privacidade pode ser definida como direito de discrição das informações pessoais ou, conforme o jurista estadunidense Louis Brandeis, corresponde literalmente ao direito de ser deixado em paz (*the right to be let alone*), e se delimita em contraposição com a vida pública, vista e conhecida pelos demais sujeitos sociais. No entanto, existem certos aspectos da vida privada que interagem diretamente com a vida pública e, neste sentido, cite-se ato de violência praticado por um representante de Estado contra seu cônjuge ocorrido dentro de sua residência. O fato refere-se a características do comportamento moral e pode influenciar nas práticas de políticas públicas voltadas ao combate da violência contra a mulher. Há, então, o evidente interesse do público de acesso à informação intrínseco à escolha de seus representantes políticos. Por isso é necessário ponderar se a informação veiculada consiste em restrição do direito à reserva da intimidade ou diz a respeito fatos de interesse social.

As relações sociais foram transportadas para o meio virtual de modo que a vida privada dos indivíduos sofre alta exposição nas redes sociais o que alterou sobremaneira os perímetros da privacidade.

As finalidades social e econômica determinantes do advento dos direitos fundamentais de primeira dimensão representam a fronteira jurídica e ética destes últimos não sendo correto afirmar que tenham de ser protegidos ou tratados como direitos absolutos, não obstante seu caráter axiológico, servindo como base jurídica para o ordenamento constitucional. Em caso de tensão entre direitos fundamentais cabe a ponderação de princípios haja vista a proteção da sociedade e a segurança jurídica das normas constitucionais. Dessa forma, quando há conflito entre a inviolabilidade do sigilo de dados, relacionado com a proteção à vida privada – e, por vezes, à intimidade – e o direito à informação, que pode ser diretamente relacionado com a

[8] Ferraz Jr, Tércio Sampaio. Sigilo de dados: o Direito à privacidade e os limites à função fiscalizadora do Estado, 2011. Disponível em.: < http://www.terciosampaioferrazjr.com.br/?q=/publicacoes-cientificas/28>. Acesso em: 08 set. de 2018

liberdade de expressão e transparência com acesso às tecnologias, o princípio de maior peso é aplicado em detrimento ao de menor valor de acordo com a conjuntura jurídica, social e econômica da situação.

Mas como definir qual desses princípios deve prevalecer quando na sociedade da informação ocorre alta exposição da vida privada por escolha pessoal? Os espaços públicos e privados se distinguem conforme a destinação dada pelo ser coletivo ou individual, com a determinação de preceitos de eliminação de antíteses entre elementos que pertencem ao público e ao privado. No entanto a tarefa de discernir entre essas duas esferas não é simples, pois na sociedade da informação ocorre constante redefinição da fronteira entre os dois espaços por haver alta interação entre eles. Isso se dá devido à rapidez e acessibilidade das tecnologias de comunicação às atividades cotidianas, criando um ambiente no qual os indivíduos são vigilantes e vigiados em tempo real. E as atividades cotidianas podem influenciar sensivelmente o grau de exposição pública quando os dados não são corretamente manipulados.

A privacidade tem como aspecto primordial a proteção de dados pessoais, já reconhecido como elemento fundamental pelo Conselho de Direitos Humanos da Organização das Nações Unidas (CDHONU), previsto no art. 17 do Pacto Internacional sobre Direitos Civis e Políticos (PIDCP), complementado, *à posteriori*, pelo Comentário Geral nº 16, da Compilação de Instrumentos Internacionais de Direitos Humanos [9], que versa sobre a necessidade de proteção de dados pessoais:

> "A coleta e a manutenção de informações pessoais em computadores, bancos de dados e outros dispositivos, seja por autoridades públicas ou entidades privadas, devem ser reguladas por lei. Medidas eficazes devem ser tomadas pelos Estados para garantir que as informações relativas à vida privada de uma pessoa não cheguem às mãos de pessoas que não são autorizadas por lei a recebê-las, processá-las e usá-las, e nunca serão usadas para fins incompatíveis com o Pacto".

Assim, infere-se a partir do excerto que a vida humana é a razão de existir dos direitos e garantias fundamentais consagrados pela Constituição Brasileira que, ao tratar do direito à

[9] Brasil. Senado Federal. Parecer quanto aos Projetos de lei n°330/2013, 131/2014 e 181/2014. p.4 *apud http://www.refworld.org/docid/453883f922.html*. Disponível em: <file:///C:/Users/CL%20PC/Downloads/DOC-Relat%C3%B3rio%20Legislativo%20-%20SF175648629127-20171003%20(1).pdf> Acesso em: 08 de set. 2018.

dignidade da pessoa humana no qual se acha incrustada a proteção à privacidade, entrou em sintonia com os tratados internacionais de Direitos Humanos e trouxe um 'novo' sentido ao pensamento da sociedade acerca da proteção dos direitos fundamentais da humanidade em sincronia com outros países ratificadores.

Os direitos de primeira dimensão, dentre eles a liberdade, liberdade de expressão, privacidade, direito à vida, caracterizam-se por serem individuais e requererem a abstenção do Estado devido ao seu caráter negativo, exigindo uma obrigação de não fazer, ou seja, são utilizados pelos indivíduos como resistência às intromissões e abusos estatais na esfera privada. Surgiram em momentos diferentes conforme a necessidade de cada época e têm suas origens no raciocínio liberal-burguês e estão presentes nas primeiras constituições escritas. Efluíram de documentos históricos como a Magna Carta (1215), a Paz de Westfália (1648), o *Habeas Corpus Act* (1679), a Carta de Direitos ou *Bill of Rigts* (1688), a Declaração de Independência dos Estados Unidos (1776) e a Declaração de Direitos do Homem e do Cidadão de 1789, sendo estas duas últimas consequências das Revoluções Americana e Francesa.

Dentro deste contexto se encontram a proteção à intimidade e à vida privada cuja titularidade é atribuída ao indivíduo e se empregam contra invasões à esfera pessoal. Dessa forma, quando a Constituição da República faz referência à inviolabilidade da vida privada, da intimidade, da honra e da imagem das pessoas assegurado o direito à reparação por danos quando houver violação, reconhece que estes são espécies do gênero privacidade[10].

Não obstante ser aceito universalmente que o direito à intimidade é remédio ante a interferência estatal não há um consenso quanto aos conceitos e fronteiras e, dependendo da cultura jurídica, econômica e social de cada país, a interpretação pode ser mais específica ou mais extensa.

Assim, para seguir uma certa orientação, adota-se, no Brasil duas teorias referentes à contextualização da privacidade. A primeira, denominada teoria das esferas, tem origem germânica e adota preceitos constitucionais capazes de harmonizar princípios, além de diferenciar vida privada e intimidade como bens jurídicos diferenciados[11]. Ainda, de acordo com Szaniawski, o Tribunal Federal Constitucional Alemão (BVerfGE) aplica essas teorias em suas decisões: o grau de tutela jurisdicional é definido conforme o nível de acessibilidade da esfera pessoal, ou seja, esferas mais íntimas requerem um defesa mais intensa.

---

[10] NOVELINO, Marcelo. **Manual de direito constitucional**. São Paulo: Editora Método, 2014. p.155.
[11] SZANIAWSKI, Elimar. Direitos de personalidade e sua tutela. 2.ed. São Paulo: Editora Revista dos Tribunais, 2005.

Na teoria dos círculos concêntricos a vida privada é dividida conforme o grau de sociabilidade ou de conhecimento: a classificação parte do círculo mais íntimo para o mais susceptível de conhecimento. Segundo Heinrich Hubmann[12], a personalidade humana pode ser fracionada em três círculos. O primeiro se refere à esfera privada, a *Privatsphäre*, no qual se observa momentos condizentes apenas ao próprio indivíduo ou àqueles que o cercam e pode abranger um maior número de relações interpessoais. Nela situam-se os hábitos e costumes do indivíduo passíveis de conhecimento e interesse público. Já a esfera íntima, ou *Vertrauensphäre*, condiz a uma parte da personalidade da pessoa mais restrita que a primeira, a intimidade ou confidencialidade, cujas informações são acessíveis apenas por familiares, amigos mais íntimos e pessoas que compartilhem o sigilo profissional. A terceira esfera (secreta), *Geheimsphäre* diz respeito à unicidade do indivíduo na qual a personalidade toma forma e detém informações compartilhadas com o menor número possível de pessoas ou, simplesmente, não compartilhada. Esse círculo inclui a formação do conceito de sexualidade, religiosidade e ideologia filosófica, por exemplo, que permeiam a parte mais íntima da pessoa.

No entanto, a delimitação dos conceitos de público e privado varia conforme as características de cada pessoa, diretamente influenciadas pela cultura, economia e sociedade do meio em que vivem. Deduz-se, a partir daí, a dificuldade em se elaborar uma norma duradoura, cujo grande obstáculo é o desenvolvimento tecnológico 'imparável'.

Ademais, pode ser identificado como outro obstáculo os longos processos legislativos. Até que uma norma seja editada, tornando-se um projeto, e faça parte do ordenamento jurídico de um Estado houve a persecução de um caminho mais burocrático do que o fechamento de um negócio *on-line*. No caso brasileiro para que um projeto de lei regulador de algum aspecto do Direito Digital seja aprovado podem ser convocadas audiências públicas com especialistas da área correlata e, ainda, a tramitação por comissões das duas Casas do Congresso até que chegue ao plenário de cada uma delas, e daí até a sanção ou veto presidencial.

No que tange à identificação dos primeiros problemas trazidos pela tecnologia face à reserva da privacidade, destaque-se a obra *Privacy and Freedom* de Alan F. Westin, que apesar de não tratar do tema invasão de privacidade com utilização de tecnologia, é uma referência ao tema da teoria geral de privacidade. Segundo Westin o sistema político condiciona o equilíbrio entre a revelação e a privacidade em cada sociedade. Em estados totalitários, existe muito segredo sobre o funcionamento do regime, enquanto há forte

[12] HUBMANN, Heinrich. Das Persönlichkeitsrecht. Böhlnau – Verlag Münster / Köln, 1967.

monitoramento dos indivíduos. Costuma-se divulgar nesses regimes que a privacidade é imoral, antissocial e egoísta. Já em regimes democráticos, a publicidade é a regra de funcionamento dos governos, enquanto a privacidade é entendida como o exercício de atividades não relacionadas à vida política, conferindo oportunidades para que as pessoas tenham ideias independentes e adotem posturas críticas. No mesmo sentido, cada povo tem uma noção distinta de privacidade, mediante maior ou menor reserva nos contatos interpessoais[13].

Os estudos de Westin foram referência para o aparecimento de diversas normas mundiais com o propósito de proteger a vida particular. Uma das pioneiras a tratar sobre o tema foi a lei alemã *Hessisches Datenschutzgesetz*[14] de 1970 que inaugurou o primeiro supervisor (autoridade) de proteção de dados de que se tem notícia. Além disso estabeleceu regras quanto ao processamento de dados para fins de planejamento público, utilização de dados pessoais, mesmo sem consentimento do titular, para fins de pesquisa científica desde que o interesse público suplante o objetivo da pesquisa. Também, de acordo com a norma, o empregador poderia processar os dados de seus funcionários somente se este for o caso de início, execução, rescisão ou conclusão da relação de emprego e implementação de planejamento interno, organizacional, social de e medidas de pessoal, sendo exigido pela legislação, um acordo coletivo ou um contrato de serviço.

Na mesma esteira legislativa a Suécia elaborou o *Datalagen*, Lei 289 de 11 de maio de 1973, primeira norma do país a versar sobre proteção de dados. No mesmo ano a Assembleia Consultiva do Conselho Europeu publica uma Resolução com enfoque na proteção de dados, sendo esta proteção um pressuposto irrestrito ao direito à privacidade. Essa disposição se originou da necessidade de se relacionar a Convenção Europeia para proteção dos Direitos do Homem e das Liberdades Fundamentais (CEDH), no que concerne ao direito ao respeito à vida privada e familiar, com a questão da coleta e tratamento de dados. A resolução tinha como finalidade a adoção dos princípios mínimos de proteção de dados pelos países signatários. Na mesma linha, a França adota a Lei sobre Informática e Liberdades (*Informatique et Libertés*) em 1978. Seu exemplo foi seguido por Luxemburgo, Áustria e Dinamarca.

---

[13] FILHO, Eduardo Tomasevicius *apud* Alan F. Westin. p. 129-169. Disponível em: <http://www.producao.usp.br/bitstream/handle/BDPI/49058/Em%20dire%C3%A7%C3%A3o%20a%20um%20novo%201984.pdf?sequence=1&isAllowed=y> Acesso em: 08 set. 2018.

[14] Alemanha. *Land de Hesse*. Hessisches Datenschutzgesetz (HDSG). Disponível em <https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/content-downloads/HDSG.pdf> Acesso em 08 set. 2018

A elaboração de leis de caráter nacional influenciou e, em outros casos, antecipou a origem de normas de caráter multinacional. Uma delas surgiu em 1980 por meio do Comitê de Ministros da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) que introduziu no ordenamento econômico internacional as Diretrizes sobre Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais e fazia referência à cooperação internacional entre os países signatários e à segurança nos fluxos ininterruptos[15]. Como não possuía efeito vinculante, visto que muitos países não adotaram seu conteúdo, logo foi contornada pela Convenção 108 ou Convenção de Estrasburgo de 1981, cuja finalidade era fazer os países signatários internalizarem suas medidas e foi significativa quanto ao tratamento da proteção de dados como direito fundamental, conforme pode se inferir de seu escopo, qual seja, "garantir, no território de cada Parte, a todas as pessoas singulares, seja qual for a sua nacionalidade ou residência, o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito («protecção dos dados»)[16]". Além de obter êxito quanto a seu intento, a adoção de suas medidas nas legislações nacionais, abriu portas para a padronização efetiva quanto à segurança e fluxo de informações pessoais.

Desde então observou-se a necessidade de haver uma legislação internacional que regulamentasse a proteção de dados pessoais e seu tratamento. Uma das principais foi a Resolução n° 45/95 da ONU[17], que regula os arquivos de dados pessoais. Nela há a adoção de princípios da legalidade e justiça, da precisão, da especificação do propósito, do acesso da pessoa interessada, da não discriminação, da faculdade de fazer exceções, da segurança, supervisão e penalidades, fluxo de dados transfronteiriço e âmbito de aplicação. Interessante notar a disposição da norma sobre o desígnio, por lei de cada país ratificador, da autoridade responsável pela observância dessas diretrizes e pela aplicação de sanção em caso de inobservância das mesmas.

A evolução das leis nacionais e internacionais convergiu para a adoção de uma norma que procurasse unificar de forma geral as políticas de proteção de dados adotadas por países,

---

[15] CONSELHO DA OCDE. Organização para a Cooperação e Desenvolvimento Econômicos. Diretrizes sobre a Proteção da Privacidade e Fluxos Tranfronteiriços de Dados. Disponível em <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> Acesso em: 08 set. 2018.

[16] CONSELHO DA EUROPA. Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal. Estrasburgo – França, 1081.

[17] Organização das Nações Unidas (ONU). Diretrizes para Regulamentação de arquivos de dados pessoais informatizados, em tradução livre. ONU – Organização das Nações Unidas. Disponível em <http://www.refworld.org/docid/3ddcafaac.html> Acesso em: 22 set. 2018.

cujo ordenamento jurídico é específico sobre o tema. Em razão disso, a Diretiva 95/46/CE de 24 de outubro de 1995, adotada pela União Europeia, procurou solucionar as divergências entre os entendimentos quanto à segurança de dados pessoais, que passou a ser um preceito fundamental dos cidadãos, oficialmente.

Em relação às Américas a privacidade e proteção de dados pessoais são objeto da Resolução 186/2012, ou *Proposed Statement of Principles for Privacy and Personal Data Protections in the Americas* e a Resolução 212/2015, ou *Protection of Personal Data*[18], ambas apresentadas pela Comissão Jurídica Interamericana, com pretensão de harmonizar a regulação de segurança de dados dos países membros. O principal intento da Res. 186/2012 é a prevenção de danos ao titular dos dados quando há uso incorreto ou desnecessário de suas informações por meio da prática dos princípios estabelecidos na 80° Sessão Ordinária. Já a Res. 212/2015 aprovou o documento CJI/doc.474/15 rev.2 sobre Privacidade e Proteção de Dados Pessoais no qual consta a finalidade dos princípios da OEA/OAS: estabelecer um marco para salvaguardar os direitos das pessoas à proteção dos dados pessoais e autodeterminação em relação à informação[19].

A convergência para a unificação das legislações locais é requisito para a cooperação internacional quanto à transparência e livre fluxo de dados a fim de aperfeiçoar as parcerias políticas e comerciais. É o que se tem visto nas normas supranacionais. Dessa forma, o Regulamento Geral de Proteção de Dados (RGPD) – que será tratado em tópico específico – mesmo abrangendo, inicialmente, os países membros da União Europeia, aplica-se a todas as empresas da UE, não importando a localização. Esse é um dos fatores que a tornam uma norma com efeitos globais.

---

[18] Organization American States (OAS). *Privacy and Personal Data in the America*. CJI/Res. 186/2012 e CJI/Res. 212/2015. Disponível em <https://www.oas.org/en/sla/iajc/docs/ijc_current_agenda_privacy_personal_data_protection.pdf> Acesso em: 10 set. 2018.

19 OAS. Departamento de Derecho Internacional. *El Comité Jurídico Interamericano adopta por consenso informe sobre Protección de Datos Personales*. Disponível em <http://www.oas.org/es/sla/ddi/boletines_informativos_Proteccion_datos_personales_CJI_informe_Abr-2015.html> Acesso em: 10 set. 2018.

CAPÍTULO 2 –VIOLAÇÃO DE DADOS PESSOAIS: ALGUNS PRECEDENTES

Ao concordar com os termos de uso e políticas de privacidade, o indivíduo abdica de certos aspectos da sua intimidade (como preferências políticas, religiosas, gostos por determinado cosmético, trajetos-mobilidade, interações com familiares, cor da pele, opção sexual, gênero, amigos por aplicativos etc.) a fim de contratar serviços que atendam da melhor forma os objetivos almejados, que vão desde um simples cadastro em *sites* de relacionamento até a realização de operações comercias.

Para tanto são princípios básicos no desenvolvimento dessas relações entre o titular e o tomador de dados a transparência das operações e a garantia de que as informações pessoais permanecerão em ambiente seguro. Ocorrendo a quebra da estrutura dos sistema de segurança de dados, inevitavelmente, a credibilidade do usuário é abalado com consequências para o mercado digital de dados. Exemplifique-se a queda do valor das ações experimentada pelo Facebook quando houve o escândalo da utilização indevida de dados pela Cambridge Analytica, a fim de favorecer a campanha eleitoral de Trump e ter possível interferência no *Brexit*.

Para uma melhor compreensão sobre o impacto das violações de dados é mister citar alguns casos com repercussão nacional e internacional sobre utilização indevida e vazamento de informações, nos quais se observam as fragilidades, por vezes quase implícitas, dos sistemas de armazenamento de diversos modelos de negócios.

2.1. FACEBOOK x CAMBRIDGE ANALYTICA

Recentemente ouvimos falar sobre o vazamento de dados do Facebook e de como o fato afetou a credibilidade de milhões de usuários da rede social pelo mundo quanto à privacidade de seus dados.

O episódio ocorreu quando a Cambridge Analytica, empresa de análise de dados que atuou nas eleições para presidente dos Estados Unidos em 2016, utilizou dados psicográficos ou comportamentais, além dos demográficos, de cerca de 50 milhões de usuários para direcionar a campanha eleitoral de Donald Trump. E a principal responsável por fornecer essa informação foi a empresa de Mark Zuckerberg.

Em abril de 2010 foi lançada a plataforma Open Graph para outros aplicativos a fim de introduzir uma interação melhor do usuário da rede social e da página da web que quisesse

divulgar a partir do uso de metadados: diz respeito a um conteúdo que pode ser visualizado e compartilhado independente da página externa. Mas, para tanto, os desenvolvedores externos requeriam (como ainda requerem) permissão do usuário para ter acesso a uma quantidade de dados razoável, incluindo dados sensíveis, bem como informações pessoais da rede de amigos. Se fossem consentidas permissões adicionais, aplicativos externos poderiam acessar as mensagens pessoais dos usuários. Disso se valeu o instrumento criado por Aleksandr Koogan com o objetivo de mapear, psicologicamente, milhões de perfis do Facebook nos Estados Unidos.

A CA teve ajuda de dois professores da Universidade de Cambridge: Aleksandr Kogan e Michal Kosinski. Especialista em explorar os processos sociais e emocionais, Kogan foi responsável por desenvolver um aplicativo de teste de personalidade em forma de quiz, o *thisisyourdigitallife*[20] - ou essa é sua vida digital, em tradução livre – em 2013, que foi lançado no Facebook, ao qual 270.000 pessoas responderam em troca de compensação financeira. A alegação foi de que se tratava de uma pesquisa acadêmica utilizada por psicólogos para estudar perfis.

Para ter acesso às previsões de personalidade (entenda-se: como forma de proceder ao *login*) os usuários teriam que acessar o seu perfil no Facebook, informar a sua localização, bem como a opinião sobre o serviço e a autorização para acesso aos dados dos amigos dos "participantes da pesquisa". Esses dados foram vendidos por Kogan à Cambridge, sem autorização dos donos das informações privadas, algo contrário ao código de conduta do Facebook.

Os dados vieram com um brinde: informações sobre os amigos das pessoas que participaram do teste. Nesse ponto a atuação de Kosinski se mostra importante, pois ao usar engenharia reversa em cima dos *likes*, desenvolveu um modelo capaz de prever o perfil de personalidade dos usuários. Como a Cambridge Analytica comprou os dados desses usuários e aperfeiçoou a ideia, informações sobre os perfis de milhões de eleitores estadunidenses foram criadas com o propósito de veicular propaganda eleitoral de acordo com o perfil de cada um.

Na época em que o incidente ocorreu a política da plataforma permitia que aplicativos externos coletassem dados de amigos dos usuários. No entanto, os dados deveriam ser usados para melhorar a experiência do próprio usuário no aplicativo. Não havia controle sobre a proibição da venda de dados para propaganda. Somente a partir de 2014, as regras para acesso

[20] De acordo com a ex-funcionária da Cambridge Analytica, Britney Kaiser, outros aplicativos foram usados para coletar informações dos usuários, a exemplo do *Sex Compass*, ou Bússola sexual em tradução livre.

aos dados de amigos de usuários foram alteradas: a partir de então seria necessário permissão para essa finalidade. Mas essas alterações não foram retroativas de modo que não se excluíram os dados obtidos por Kogan.

Conclui-se que não houve invasão da rede social para roubo de dados, mas subversão à política do Facebook, com coleta não autorizada de dados a fim de direcionar propagandas eleitorais, inclusive de forma específica, para convencer eleitores indecisos. Embora os responsáveis pela rede social tenham descoberto o uso indevido de informações dos usuários em 2015, apenas no dia 16 de março de 2018 procedeu à suspensão dos perfis da Cambridge Analytica e de Aleksandr Kogan. Como consequência do escândalo a CA encerrou suas atividades nos Estados Unidos.

A trama, descoberta através de investigações realizadas pelos veículos de comunicação *The New York Times* e *The Observer*, põe à prova sobre o quão delicado é o assunto por envolver de forma direta informações de milhões de pessoas e de como elas podem ser valiosas, principalmente para definir o destino da maior economia do mundo e, dessa forma, influenciar a economia de outros países, em nítido efeito cascata. A partir do fato depreende-se como a política de privacidade da mais ampla rede social pode ser tão frágil frente a interesses político-econômicos.

2.1.1. Repercussão nos Estados Unidos

A *Federal Trade Commission* (FTC), agência federal com função de proteger os consumidores e promover a concorrência, iniciou investigações acerca da possibilidade de a rede social ter violado um acordo realizado em 2011[21] no qual se responsabilizou em adotar medidas para evitar que os dados dos usuários/consumidores fossem compartilhados e tornados públicos sem o consentimento destes. Naquela época a FTC listou alguns casos em que o Facebook não cumpria suas promessas quando assegurou a privacidade dos consumidores quanto ao acesso de terceiros às informações pessoais, quanto à inacessibilidade dos conteúdos das contas em caso de exclusão das mesmas e em relação ao não compartilhamento dos dados pessoais com anunciantes, dentre outros quesitos apontados pela Comissão.

[21] *Facebook settles FTC charges that it deceived consumers by failing keep privacy promisses*. Federal Trade Commission – Protecting America's Consumers, 2011.

O objetivo do acordo firmado pela FTC continua sendo a proibir "o Facebook de fazer qualquer outra alegação de privacidade enganosa" e exigir "que a empresa obtenha a aprovação dos consumidores antes de mudar a maneira como compartilha seus dados", bem como "que ela obtenha avaliações periódicas de suas práticas de privacidade por auditores independentes terceirizados nos próximos 20 anos" [22] . Caso haja comprovação do descumprimento do acordo por parte da empresa, esta pode arcar com uma multa de US$ 40.000,00 por usuário, e a cada dia, cujo valor total pode chegar à casa dos trilhões.

Alguns especialistas dizem que houve quebra do acordo, pois o Facebook permitia que Kogan coletasse os dados. Reforça esse fato, a declaração de Zuckerberg durante audiência no Congresso, sobre ter descoberto a venda de dados realizada por Kogan à Cambridge Analytica, motivo pelo qual solicitou a esta empresa que excluísse as informações. No entanto, o Facebook além de não verificar se a CA cumprira a determinação da exclusão, não comunicou aos usuários dos serviços da rede que seus dados haviam sido indevidamente compartilhados. Tal situação reforça a perspectiva da violação do consentimento e, consequentemente, do acordo.

Após a divulgação do uso inadequado dos perfis dos usuários do Facebook pela Cambridge, em 26 de março de 2018, o então diretor interino, Tom Pahl, confirmou a abertura das investigações e declarou[23]:

> "A FTC está firme e totalmente comprometida em usar todas as suas ferramentas para proteger a privacidade dos consumidores. Entre essas ferramentas, destaca-se a ação de imposição contra empresas que não honram suas promessas de privacidade, incluindo o cumprimento do Privacy Shield, ou que se envolvem em atos injustos que causam danos substanciais aos consumidores, violando a Lei do FTC. As empresas que tenham resolvido as ações anteriores da FTC também devem cumprir as disposições da FTC que impõem requisitos de privacidade e segurança de dados. Consequentemente, a FTC leva muito a sério as notícias recentes da imprensa levantando preocupações substanciais sobre as práticas de privacidade do Facebook. Hoje, a FTC está confirmando que tem uma investigação aberta e não pública sobre essas práticas".

De outro viés, logo após o ocorrido com o Facebook em relação ao compartilhamento não autorizado dos dados de milhões de estadunidenses, a Câmara dos Deputados e o Senado dos Estados Unidos aprovaram, sem muitos debates e tramitação, legislação acerca de dados que circulam fora da jurisdição do país, denominada *Cloud Act*, sigla para *Clarifying Lawful Overseas Use of Data Act* (ou "Lei para Esclarecer o Uso Legal de Dados no Exterior", em

[22] *Facebook settles FTC charges that it deceived consumers by failing keep privacy promisses*. Federal Trade Commission – Protecting America's Consumers, 2011.

[23] Disponível em < https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection> Acesso em: 20 de set. 2011.

tradução livre)[24]. Segundo a norma, aprovada em 23 de março de 2018, empresas de tecnologia que funcionem nos Estados Unidos são obrigadas a fornecer, mediante intimação ou mandado, dados armazenados em solo nacional ou em território estrangeiro a fim de contribuir com investigações criminais. O provedor de serviços eletrônicos pode contestar a ordem se entender que as informações requeridas são de pessoas de outra nacionalidade ou quando o requerimento for de encontro à legislação do país de origem dos dados solicitados. Por este último motivo, a legislação prevê que haja acordos entre os Estados Unidos e outros países.

Essa norma busca adequar a exigência de mandado de busca, prevista na Quarta Emenda[25] da Constituição dos Estados Unidos, para retenção de informações contidas em provedores de serviços de comunicação a fim de fomentar investigações criminais. Algumas entidades de proteção à privacidade, no entanto, são contrárias à 'Lei da Nuvem', pois permite o compartilhamento de dados com países que transgridem direitos humanos, bem como permite que estes acessem os dados armazenados sob jurisdição norte-americana.

Nos Estados Unidos não há, ainda, uma lei geral para a proteção de dados pessoais, embora haja legislação fragmentada que dispõe, por exemplo, sobre a Lei de Privacidade de Comunicação Eletrônica (*Electronic Communications Privacy Act of 1986* – EPCA), recém atualizada pela Lei de Nuvem, e sobre a proteção da privacidade de crianças (*Children's Online Privacy Protection Act of 1998* – COPPA). Enquanto isso não ocorre, vários Estados norte-americanos incorporaram em sua legislação local normas para a proteção de informações pessoais, principalmente após a entrada em vigor do Regulamento Geral de Proteção de Dados Europeu (RGPD).

Na Califórnia foi aprovada em 28 de junho de 2018 a Lei de Privacidade do Consumidor da Califórnia de 2018, dando aos moradores mais controle sobre seus dados processados por empresas de tecnologia. Conforme a Lei, que entra em vigor em 01° de janeiro de 2020, um dos motivos da aprovação foi, justamente, o uso indevido de dados pela Cambridge Analytica. A partir de então, os consumidores do Estado passaram a ter a garantia de salvaguardas contra o uso indevido de suas informações pessoais. Ademais, as empresas devem fornecer informações, sempre que solicitadas por um californiano, sobre quais dados são coletados, pra quem são vendidos e onde são divulgados, bem como de praticar os

[24] ESTADOS UNIDOS. Congresso dos Estados Unidos da América. HR4943. 115° Congresso do Cloud Act (2017-2018).

[25] "O direito do povo à inviolabilidade de suas pessoas, casas, papéis e haveres contra busca e apreensão arbitrárias não poderá ser infringido; e nenhum mandado será expedido a não ser mediante indícios de culpabilidade confirmados por juramento ou declaração, e particularmente com a descrição do local da busca e a indicação das pessoas ou coisas a serem apreendidas".

mesmos preços e serviços para os que exercem o direito à privacidade, algo bem semelhante aos dispositivos do RGPD.

Outro ponto relevante é a elevação do limite de idade adotado para a proteção de menores em relação ao compartilhamento de seus dados: diversamente da idade adotada pela legislação nacional, as pessoas com idade entre 13 e 16 anos só podem ter seus dados vendidos mediante seu consentimento. Já os menores de até 13 anos necessitam do consentimento dos pais. Caso haja violação de dados a indenização chega a US$ 750,00 por ato infracional.

Praticamente, todos os Estados optaram por leis de notificação e violação de dados, nas quais empresas devem notificar os consumidores sobre possível comprometimento de suas informações pessoais. A exemplo disso, cite-se: (1) a Luisiana (Lei n° 382 - *Breach Notification Law*), segundo a qual os residentes do Estado devem ser notificados em até sessenta dias sobre violação da segurança de seus dados, (2) o Oregon (SB 1551 2018) cuja legislação atualizada requer a notificação do consumidor usuário no prazo de quarenta e cinco dias além de proibir entidades de fornecerem serviços de monitoramento de credito gratuito mediante a apresentação do número do cartão magnético e (3) Iowa (*House File 2354 - Relating to Student Personal Information Protection Act*), cujos destinatários são provedores de *sites* e aplicativos destinados à educação de estudantes no que tange à proibição de usar informações do aluno para venda ou aluguel além de exigir que as empresas implementem e mantenham serviços de segurança de dados.

Por parte dos usuários e investidores, o escândalo da venda de dados do Facebook desacreditou fortemente a rede social, que chegou a ter um déficit de trinta bilhões de dólares em ações, e abriu os olhos para a falta de privacidade da rede, principalmente quanto à monetização do produto "você".

2.1.2. Repercussão na União Europeia

Com o vazamento de dados de 2,7 milhões de europeus[26] no bloco de 28 países, muitas autoridades da U.E. anunciaram a abertura de investigações contra o Facebook. Diante disso o Parlamento Europeu convidou Mark Zuckerberg a prestar esclarecimentos acerca da proteção dada pela rede social aos usuários.

[26] UOL notícias. Facebook confirma vazamento de dados de 2.7 milhões de usuários europeus. 06 abr. 2018.

Diante dos parlamentares europeus, em Bruxelas, o *CEO* foi questionado sobre a obediência da empresa quanto às novas regras do Regulamento Geral de Proteção de Dados[27], sobre uma possível compensação aos europeus que tiveram suas informações privadas expostas de forma inadequada, se o Facebook tem preconceito relativo a posicionamento conservador e foi posto à prova em relação à suspeita de a empresa ter o monopólio da comunicação social instantânea, visto que detém outras plataformas interligadas (Whatsapp e Instagram) à prestação de serviços, sem potenciais concorrentes.

Como resposta, em relação ao monopólio, Zuckerberg sustentou que o segmento no qual atua o Facebook é bastante competitivo, prometendo fornecer informações financeiras a fim de colaborar com as autoridades europeias antitruste. Já quanto à questão do preconceito político, o *CEO* afirmou que as pessoas são livres para utilizar os serviços da rede quanto à divulgação de qualquer pensamento político, sem quaisquer interferências (‘hackeamento’) para cercear orientações políticas.

Os atos de violação à privacidade das contas do Facebook teriam influenciado, também, o resultado do Brexit (abreviação para *Britain Exit*, ou saída britânica) que culminou com a votação favorável à saída do Reino Unido da União Europeia, segundo Christopher Wylie, ex-diretor de pesquisa da Cambridge Analytica. Como consequência, a saída do Reino Unido pode causar uma conturbada revisão das leis europeias vigentes no território britânico, visto que, conforme a necessidade, algumas seriam absorvidas ou atualizada e outras revogadas. No âmbito econômico, o Reino Unido é responsável por contribuir com 11,3 bilhões de euros ao bloco, sendo uma das principais bases para a economia ao lado da França e Alemanha. De outro lado, o prejuízo para o Reino Unido seria o pagamento de uma multa estimada entre 60 e 100 bilhões de euros, um valor praticamente impagável.

Alguns meses após a venda de dados do Facebook, a empresa foi multada pelo *Watchdog Information Commissioner's Office* (ICO), órgão regulador do Reino Unido, no valor de US$ 664.000,00 (seiscentos e sessenta e quatro mil dólares) pelo manuseio indevido de informação pessoal de milhões de pessoas sem autorização. Como fundamentos para a sanção estão a falta de proteção adequada à privacidade dos usuários e a pouca importância dispensada à coleta indevida dos dados pela CA. Caso o Facebook tivesse tomado as providências cabíveis, não haveria manipulação para fins políticos e, possivelmente, o Reino Unido continuaria a fazer parte da UE[28].

---

[27] A audiência perante o Parlamento Europeu ocorreu em 22/05/2018, três dias antes de o RGPD entrar em vigor.
[28] Romm, Tony; Dwoskin, Elizabeth. Facebook is slapped with first fine for Cambridge Analytica scandal. The Washington Post. Business. Publicado em 10 jul. 2018.

Ademais, ressalte-se que os Estados membros da União Europeia subscrevem a Convenção Europeia de Direitos Humanos (CEDH) e estão submetidos ao entendimento do Tribunal Europeu de Direitos Humanos. Quanto ao artigo 8° da Convenção[29], o Tribunal deu entendimento amplo, sendo de grande relevância o direito à privacidade dos dados na comunidade europeia, principalmente quando se trata do compartilhamento entre os países do bloco.

Cabe mencionar que a Diretiva 95/46/CE, "aplicável a todos os tratamentos de dados pessoais nos Estados-Membros, nos setores público e privado[30]", vigia na época em que os dados de usuários do Facebook foram vendidos à Cambridge Analytica, mas foi revogada pela Diretiva 2016/680 e pelo Regulamento Geral de Proteção de Dados europeu – a ser tratado posteriormente – aprovados pelo Parlamento Europeu e do Conselho. O motivo da revogação se trata de sua não aplicação "ao tratamento de dados pessoais no exercício de atividades não sujeitas à aplicação do direito comunitário, como as atividades realizadas nos domínios da cooperação judiciária em matéria penal e da cooperação policial[31]".

Tratando-se a inviolabilidade de informações privadas dos cidadãos europeus como algo inerente à proteção aos direitos da personalidade, a *Irich Data Protection Comissioner* (DPC), ou Comissão de Proteção de Dados da Irlanda, responsável por investigar a rede social em nome da União Europeia, abriu investigação formal para averiguar a extensão da responsabilidade da rede sobre a quebra do sigilo das informações dos cidadãos europeus envolvidos. Segundo a DPC "a investigação examinará a conformidade do Facebook com sua obrigação sob o RGPD de implementar medidas técnicas e organizacionais apropriadas para garantir a segurança e a proteção dos dados pessoais que processa.[32]"

Outra autoridade europeia, o órgão antitruste alemão Federal Cartel Office (FCO), que deu início às investigações contra a prática de coleta de dados pela rede social em 2016, busca saber como o Facebook adquire dados de aplicativos de terceiros, sendo Whatsapp e o

[29] A CEDH foi elaborada pelo Conselho da Europa (CdE) a fim de incentivar os direitos humanos, a democracia e o Estado de Direito em resposta aos atos desumanos oriundos da Segunda Guerra Mundial e tem o Tribunal Europeu de Direitos Humanos (TEDH) como autoridade *fiscalizadora* do cumprimento dos princípios da CEDH. Segundo o art. 8°, *1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem - estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros*. Fonte: <https://www.echr.coe.int/Documents/Convention_POR.pdf>

[30]União Europeia. Parlamento Europeu e Conselho da União Europeia. Diretiva 2016/680, de 27 abr. 2016. Jornal Oficial da União Europeia. Bruxelas/BZ. 2016.

[31] Idem.

[32] HALPIN, Padraic. *Facebook's lead EU regulator opens probe into data breach*. *Cyber Risk.* Reuters.03 out. 2018. Disponível em: <https://www.reuters.com/article/us-facebook-cyber-ireland/facebooks-lead-eu-regulator-opens-probe-into-data-breach-idUSKCN1MD2EC> Acesso em: 10 out. 2018.

Instagram incluídos. A justificativa para esta decisão foi a de que a empresa, além de seguir a atividade *on-line* dos usuários de seus serviços, também tinha conhecimento das atividades daqueles que não utilizavam a rede.

2.1.3. Repercussão no Brasil

No Brasil, as declarações de Mark Zuckerberg ao Congresso dos Estados Unidos sobre o mau uso de dados dos usuários, ensejou Ação Civil Pública ajuizada pela entidade SOS Consumidor[33] põem razão da violação de dados de cerca de 443 mil usuários brasileiros, requerendo reparação por danos morais no valor de 10 milhões de reais, pois entende que o Código de Defesa do Consumidor se aplica por considerar que os usuários são consumidores e a rede social uma fornecedora e prestadora de serviços.

Devido à obtenção indevida de informações pessoais o Departamento de Proteção de Defesa do Consumidor, órgão integrante da Secretaria Nacional do Consumidor (SENACON), notificou o Facebook a fim de obter respostas quanto à venda dessas informações e em relação à quebra de seu sigilo. Além disso, informações como o número exato de usuários afetados e se houve consentimento para a captura de dados foram solicitados. O prazo estipulado foi de 10 dias.

Ainda, a Comissão de Proteção dos Dados Pessoais da 1ª Promotoria de Justiça de Defesa do Consumidor do MPDFT abriu investigação para apurar se os dados de brasileiros foram atingidos e quantos sofreram exposição. O inquérito, instaurado pela Portaria n° 2/2018, classificou como interessados a Cambridge Analytica, a Ponte Estratégia Planejamento e Pesquisa LTDA[34], Facebook Serviços Online do Brasil LTDA, Facebook Miami, INC, Facebook Global Holding III, LLC e Usuários brasileiros do Facebook.

Em 18 de abril de 2018 a Comissão Especial sobre Tratamento e Proteção de Dados Pessoais, da Câmara dos Deputados, decidiu analisar a utilização indevida de informações privadas pela Cambridge Analytica. A comissão tinha responsabilidade sobre o PL 4.060/2012 e apensados, posteriormente convertido em PL 53/2018 ao tramitar no Senado

[33] OLIVEIRA, Mariana. Associação pede indenização de R$ 10 mi ao Facebook por vazamento de dados. Conjur. 20 de abril de 2018. Disponível em: <https://www.conjur.com.br/2018-abr-20/associacao-indenizacao-facebook-vazamento-dados> Acesso em: 01 dez. 2018.

[34] Também conhecida como Cambridge Analytica Ponte. A empresa tinha como objetivo implantar o mesmo modelo de atuação da Cambridge Analytica, executado na campanha eleitoral de Donald Trump, nas eleições de 2018, no Brasil. Vide: O marqueteiro brasileiro que importou o método da campanha de Trump para usar em 2018. El País. São Paulo. 15 out. 2017.

Federal. Seu trabalho levou à aprovação da Lei 13.709/2018 que dispõe sobre tratamento, transmissão e proteção de dados pessoais.

2.1.4. Outras ocorrências

Em setembro de 2018 ocorreu novo vazamento, dessa vez de cerca de 50 milhões de pessoas, devido a uma falha interna do código do sistema em relação à maneira como outros usuários veem o perfil. Como o Regulamento Geral de Proteção de Dados Europeu já estava em vigor, a rede social comunicou às autoridades responsáveis pela proteção de dados das localidades envolvidas e invalidou os *tokens*[35] de quase 50 milhões de pessoas, além de restringir o acesso de outros 40 milhões de contas.

Não obstante os casos anteriores e a oscilação na credibilidade da manutenção do sigilo de informações pessoais, outro vazamento ocorreu[36]: hackers russos violaram o sigilo de 81 mil contas de usuários, aproximadamente. O vazamento descoberto pela BBC, com amparo na investigação realizada pela empresa de segurança Digital Shadows, traz informações variadas, inclusive mensagens entre usuários de caráter íntimo. As contas prejudicadas foram em maior parte da Ucrânia e da Rússia, mas havia conteúdos de várias geolocalizações. As contas eram comercializadas por US$ 0,10 até o início das investigações, quando, então, o anúncio saiu de circulação.

Ambas as situações evidenciam o quão frágil é o tratamento de dados frente às habilidades desenvolvidas por hackers/crackers em quebra de sigilo de informações e posterior divulgação delas, caso a vítima não cumpra as exigências.

[35] Sobre o conceito de *token* de acesso do Facebook: <https://developers.facebook.com/docs/facebook-login/access-tokens/?locale=pt_BR> Acesso em: 05 nov. 2018

[36] O fato foi levado a conhecimento público em 01 de novembro de 2018, quase dois meses após os primeiros sinais de violação serem detectados.

2.2. O BANCO INTER E A RESPONSABILIDADE PELO ARMAZENAMENTO DE DADOS SENSÍVEIS

Em abril de 2018 ocorreu o vazamento de informações pessoais de correntistas da *fintech*[37], a primeira a abrir capital na Bolsa Valores brasileira, com estímulo a outras *startups* a listarem suas ações. Os fatos chegaram a público por meio da revista digital TecMundo que recebeu mensagem eletrônica de um *hacker* autodenominado "John", contendo um manifesto de 18 laudas, no qual havia um arquivo com informações de 40 gigabytes (GB), sendo 30 GB relativos aos clientes da instituição. Por esse motivo foi inevitável a revogação do certificado digital. Segundo "John", os dados pertencem a mais de 300 mil pessoas.

O motivo do ataque foi extorquir a *fintech*[38] para que as informações continuassem em sigilo. Como o banco não acatou os termos da extorsão, em que agiu corretamente, os dados dos clientes logo foram divulgados e postos à venda pelo valor de 10 bitcoins[39]. As informações podem ser encontradas na *Deep Web*, cuja divulgação é atribuída a um grupo de *hachers/crackers* chamado "John Carter". Perturbadora é a quantidade de dados sensíveis extraídos dos arquivos das bases do Banco que cuidam de transações com cheques, senhas de cartões de crédito, dados cadastrais, conforme segue:

> – "Dados cadastrais, incluindo código de segurança e senha, de todos os quase 400.000 clientes e correntistas do Banco Inter (o TecMundo encontrou 81 mil);
>
> – Base de cadastro Mastercard com cadastro completo, incluindo e-mails, telefones, endereço, nome do pai, nome da mãe, documentos, telefone fixo e celular;
>
> – Senha dos cartões Mastercard, usados para débito, crédito, para segundo fator de autenticação de transações como pagamentos de TED e pagamento de boletos;
>
> – Fluxo de troca de senha do cartão Mastercard, incluindo senha antiga e senha nova, de todos os clientes, coletado por mais de um mês — "e que ainda está sendo coletado nesse momento";

[37] "São, na prática, intermediárias de operações *peer-to-peer* (ponto a ponto), em que pessoas aplicam dinheiro de um lado, e empresas ou outras pessoas físicas pegam empréstimo, de outro".
[38] Termo oriundo de "financial technology".
[39] Na época, 1 bitcoin valia cerca de R$ 33.000,00 (trinta e três mil reais).

> – Todos logs transacionais de todas as operações e transações bancárias realizadas por todos os clientes, incluindo valor, conta origem, conta destino a partir de fevereiro, e com algumas recuperações de janeiro;
>
> – Todas as transações, sem exceção, realizadas pelo CD Pro (o que eles chamam de conta corrente profissional, mas que na prática é apenas a conta digital PJ, pessoa jurídica). "Como esse sistema já nasceu na AWS, o histórico deles é muito maior, e eu copiei todas as transações de junho de 2017 até março de 2018", adicionou;
>
> – Todos os documentos e contratos de serviço, em formato pdf e tiff (imagem), incluindo CPF, RG, CNH, comprovantes e, eventualmente, declaração de imposto de renda para aqueles que pedem crédito ou aumento de limite do crédito;
>
> – Centenas de fotografias em formato tiff de cheques de clientes diversos usados pelo serviço de compensação de cheques por imagem no aplicativo;
>
> – Padrões de url de sistemas no cloud front;
>
> – Usuário e senha de FTP do banco Inter na empresa processadora de cartões conductor;
>
> – Dump de todos os arquivos e dados do FTP do conductor;
>
> – Chaves de API e urls usadas para validar a senha master na processadora de cartões fast solutions;
>
> – Chaves privadas ec2 usadas na AWS, chaves ssh, chaves de API de serviços e até chave privada do certificado ssl wildcard "em produção nesse exato momento";
>
> – Senhas de diversos funcionários da Virtual Sistemas e grupo Magnus, empresas terceirizadas do banco Inter;
>
> – Código fonte do novo core banking[40]".

Esse tipo de falha faz questionar a tecnologia de computação em nuvem (*cloud computing)* utilizada pelo banco para migração dos dados dos clientes, em parceria com a Amazon Web Services (AWS). O próprio grupo "John Carter" afirmou que o vazamento se tratava de "um problema grande o suficiente para comprometer não só o *rating* (avaliação) do Banco Inter frente ao Banco Central, mas comprometer o *rating* de todos os bancos digitais, ou bancos clássicos que planejem adotar soluções de *cloud computing* em grande escala".

[40] Informações conforme a revista digital TecMundo. Disponível em https://www.tecmundo.com.br/seguranca/129811-exclusivo-vazam-dados-400-mil-clientes-banco-inter.htm Acesso em 08 set. 2018.

Embora a instituição tenha confirmado a tentativa de extorsão e negado o vazamento de informações pessoais, principalmente de dados sensíveis, a TecMundo confirmou o vazamento de pelo menos cerca de 80.000 pessoas, na época, pois por meio de contato telefônico, obtido no arquivo anexado ao *e-mail*, entrou em contato com os clientes da *fintech*.

A Comissão de Proteção de Dados Pessoais do Ministério Público do Distrito Federal e Territórios (MPDFT) instaurou inquérito n° 08190.097749/18-95 para verificar se os dados comprometidos realmente pertenciam a clientes da instituição e concluiu pela responsabilidade do Banco quanto à insuficiente governança das informações de seus clientes e não clientes, posto que pessoas clientes de outros bancos que realizaram operações envolvendo o Banco Inter também tiveram seus dados expostos. Durante esta fase houve exposição pública de uma chave privada e de um certificado digital (*Anexo 2*) [41] , posteriormente revogado pela própria instituição financeira.

Em vista do resultado da investigação, a Ação Civil Pública (ACP) por danos morais coletivos[42] foi proposta com o objetivo pedagógico de fazer com que instituições usuárias de tecnologias de *cloud computing* aprimorem a segurança de aplicativos, políticas de acesso e governança de dados, pois a violação de dados de usuários, principalmente quando envolvem recursos financeiros, não mais é visto como mero 'acidente de percurso': as informações em mãos erradas geram insegurança para a economia digital e prejuízos à privacidade dos consumidores que confiaram na prestação de serviços da instituição, agindo de boa-fé. Dessa forma, apesar de a ação ser direcionada ao Banco Inter, a AWS em conjunto com o banco tem responsabilidade solidária quanto à segurança dos aplicativos e infraestrutura de identidade, pois é a detentora da plataforma onde eram armazenados os servidores e aplicações[43]. E nada obsta que haja uma ação regressiva por parte do banco contra a AWS nos moldes da ação movida contra a Target pelas instituições financeiras que se sentiram prejudicadas

[41] Pastebin. Disponível em http://pastebin.xyz/p?q=Vm9iVWw. Acesso em 22 set. 2018.
[42] Consultor Jurídico. Garantia de Segurança. MP-DF pede a condenação de banco por vazamento de dados pessoais de clientes. 31 jul. 2018. Disponível em https://www.conjur.com.br/dl/mp-df-condenacao-banco-inter-vazamento.pdf. Acesso em 22 set. 2018.
[43] Segundo o próprio superintendente de tecnologia do Banco Inter, Guilherme Ximenes de Almeida, a AWS foi selecionada "porque acreditamos no ganho de agilidade proporcionada por ela, provendo infraestrutura imediatamente quando necessário e escalável automaticamente, além de, com a estruturação de data centers distribuídos, nos permitir criar uma arquitetura de alta disponibilidade com segurança". Disponível em http://www.executivosfinanceiros.com.br/cloud/5963-banco-inter-realiza-transformacao-digital-com-cloud-computing. Acesso em 22 set. 2018.

financeiramente com o vazamento de informações dos cartões magnéticos, nomes, endereços, números de telefone de clientes de diversos bancos[44].

Conforme a própria ação proposta pelo MPDFT, o Código de Defesa do Consumidor pode ser aplicado no que pertine "à reparação de danos patrimoniais e morais, individuais, coletivos e difusos[45]".

Em recente acórdão proferido pelo Min. Antonio Carlos Ferreira, as empresas responsáveis pela prestação de serviços para fornecimento de cartão magnético e cobrança de dívidas são solidariamente responsáveis pelo defeito na prestação de serviços que redunda em cobrança indevida:

> RECURSO ESPECIAL Nº 1.749.804 - SP (2018/0150984-0) RELATOR : MINISTRO ANTONIO CARLOS FERREIRA RECORRENTE : BANCO DO BRASIL S/A ADVOGADOS : NEI CALDERON - SP114904 MARCELO OLIVEIRA ROCHA - SP113887 FABIANO ZAVANELLA - SP163012 MARCOS TRINDADE JOVITO E OUTRO (S) - SP119652 RECORRIDO : MARCELO RODRIGO DE ASSIS ADVOGADO : MARCELO RODRIGO DE ASSIS - SP133430 INTERES. : ATIVOS S.A. SECURITIZADORA DE CREDITOS FINANCEIROS ADVOGADOS : LUIZ FERNANDO MAIA - SP067217 ALAN AZEVEDO NOGUEIRA - SP198661 ALBERTO QUERCIO NETO - SP229359 PAULO HENRIQUE ZAMBON FRÓES E OUTRO (S) - SP344573 DECISÃO Trata-se de recurso especial interposto com fundamento no art. 105, III, a, da CF, contra acórdão do TJSP assim ementado (e-STJ fl. 250): AÇÃO DECLARATÓRIA CUMULADA COM INDENIZAÇÃO - Inexigibilidade de débito - Responsabilidade dos corréus configurada, nos termos dos artigos 7o, parágrafo único, e 14 do CDC - Risco da atividade, que não pode ser transferido ao consumidor - Inocorrência de culpa exclusiva do consumidor - Relação de consumo caracterizada - Aplicação do CDC - Negativação de débito declarado inexistente - Réus que não comprovaram a existência de fato impeditivo, modificativo ou extintivo do direito do autor nos termos do art. 333, II, do CPC - Responsabilidade do fornecedor apenas passível de ser afastada nas hipóteses do § 3o do art. 14 do CDC - Inocorrência de qualquer das situações de exclusão de responsabilidade - Dano moral configurado, diante do acervo probatório - Sentença de procedência mantida - RECURSO DO BANCO RÉU DESPROVIDO. AÇÃO DE INDENIZAÇÃO POR DANOS MORAIS - Negativação indevida - Dano moral configurado - Valor da indenização fixado em R$ 6.000,00 que se apresenta abaixo do devido - Valor majorado para R$ 15.000,00, que se mostra adequado à espécie - RECURSO ADESIVO DO AUTOR PROVIDO. O recorrente, em suas razões (e-STJ fls. 260/267), aduz violação dos arts. 186 e 188, I, do CC/2002, afirmando que "é seu

[44] O responsável pelo vazamento de dados foi um *malware* desenvolvido por um adolescente russo de 17 anos. O projeto foi vendido para cerca de 40 grupos criminosos, localizados, principalmente, no leste europeu. A partir daí relatos de compras não reconhecidas aumentaram e ações contra os bancos dos quais eram clientes as pessoas afetadas foram propostas. Além do mais, os bancos tiveram custos na emissão de novos cartões.

[45] Disponível em https://www.conjur.com.br/dl/mp-df-condenacao-banco-inter-vazamento.pdf. Acesso em 22 set. 2018.

> direito efetivar a cobrança dos débitos inadimplidos, por qualquer meio que seja, não havendo quaisquer indícios de irregularidades nos Contratos firmados entre as partes" (e-STJ fl. 264). Requer, ao final, a fixação da correção monetária e dos juros de mora a partir do arbitramento. O recorrido, em contrarrazões (e-STJ fls. 274/279), pugna pelo desprovimento do recurso. O especial foi admitido pelo Tribunal de origem (e-STJ fls. 317/318). É o relatório. **Decido**. Quanto ao termo inicial da correção monetária e dos juros de mora, o recorrente deixou de indicar nas razões recursais de forma inequívoca e vinculada os dispositivos de lei federal eventualmente violados pelo acórdão impugnado, fato que caracteriza deficiência na fundamentação recursal, a teor da Súmula n. 284 do Supremo Tribunal Federal. O Tribunal de origem, à luz das provas dos autos, concluiu pela responsabilidade civil da parte recorrente, nos seguintes termos (e-STJ fls. 255/257): No caso em discussão, deve ser mantida a procedência do pedido de declaração de inexistência de débito, uma vez que restou plenamente demonstrada que **a cobrança exorbitante pelo banco se deu de modo fraudulento (clonagem de cartão)**. O BANCO DO BRASIL S/A limita-se a alegar que não cometeu qualquer ato ilícito a ensejar a indenização pelos danos morais. Todavia, **contribuiu para a ocorrência do dano ao autor, juntamente com a ré ATIVOS S/A**. Conforme o art. 7º, parágrafo único, CDC: "**Tendo mais de um autor a ofensa, todos responderão solidariamente pela reparação dos danos previstos nas normas de consumo**". **A responsabilidade solidária advém do risco da própria atividade, risco consagrado também pela doutrina nacional para assegurar a reparação de prejuízos que possa causar aos usuários dos seus serviços**. (...) Sobre ser solidária, também é objetiva, nos termos do art. 14 do Código de Defesa do Consumidor. Pela "Teoria do Risco Profissional", devem os réus responder pelos maus serviços prestados, independentemente de dolo ou culpa. (*grifo nosso)*
>
> (...)
>
> (STJ - REsp: 1749804 SP 2018/0150984-0, Relator: Ministro ANTONIO CARLOS FERREIRA, Data de Publicação: DJ 25/09/2018)

Dessa forma, pode-se entender como solidárias pela prestação de serviços fornecidos pela instituição financeira 100% digital, o próprio Banco Inter e a AWS, fornecedora da plataforma na qual funcionavam as operações digitais. Ainda, as informações que transitam pelos bancos de dados de empresas que prestam serviços por *cloud computing* correm maior risco de violação devido ao grau de periculosidade e vulnerabilidade do usuário dos serviços, em claro dissenso com o princípio básico do consumidor quanto à proteção à segurança no fornecimento de serviços perigosos ou nocivos (art. 6°, I).

2.3. UM CASO PECULIAR: DECOLAR.COM E A DISCRIMINAÇÃO DE NACIONALIDADE POR *GEO PRICING* E *GEO BLOCKING*

O uso indevido de dados não se restringe apenas a invasões de terceiros em um sistema com falhas de segurança objetivando receber algum recurso, principalmente financeiro, com o repasse das informações pessoais através de dispositivos de armazenamento ou da rede mundial de computadores (neste caso, em sua camada mais profunda). O ato de beneficiar a si mesmo em detrimento dos dados alheios pode partir do próprio responsável pelo tratamento e armazenamento dessas informações.

A manipulação de informações solicitadas pelo usuário se dá de acordo com os rastros digitais deixados nos endereços eletrônicos que visita como o último *site* acessado, o endereço IP do computador, o navegador utilizado, o sistema operacional, idioma, informações de *login*, senha. Para tanto, esses dados são repassados por *cookies* aos *site* requisitado. *Cookies* são arquivos de texto responsáveis por coletar informações e preferencias do cliente, bem como as credenciais do sistema. Não se sabe qual o destino delas, tão somente a finalidade "oficial" da coleta: dedicar ao consumidor uma melhor experiência. A falta de clareza representa desvantagem, pois há o risco de ocorrer danos quanto ao valor da prestação de serviços ou compra de produtos, por exemplo.

Para atender a clientes interessados em assistir os jogos olímpicos do Rio de Janeiro a Decolar.com ofereceu hospedagens por valores diferentes a depender da localização da pessoa. Por esse motivo o Ministério Público do Rio de Janeiro (MPRJ) propôs ação civil pública por discriminação quanto à origem. Explique-se: as tarifas de hotéis e passagens aéreas para certos destinos eram mais altas para consumidores cujo endereço IP era identificado como brasileiro do que para argentinos e estadunidenses. A empresa de comércio eletrônico utilizou as práticas de *geo bloking* e *geo pricing*. A primeira consiste no bloqueio de ofertas considerando-se a geolocalização do cliente; a segunda diz respeito à precificação do serviço/produto também com base na origem geográfica.

A atuação do MPRJ foi no sentido de atender aos interesses coletivos da sociedade, pois como explícito na própria petição [46], trata-se de um "(...) caso de transgressão coletiva por parte de uma empresa de comércio eletrônico e de lesão ao

[46] MP/RJ acusa Decolar.com de manipular preços para discriminar brasileiros. Migalhas. 07 de fev. de 2018. Disponível em <https://www.migalhas.com.br/Quentes/17,MI273955,91041-MPRJ+acusa+Decolarcom+de+manipular+precos+para+discriminar+brasileiros>. Acesso em: 22 de set. 2018.

direito de uma massa de consumidores, sendo absolutamente imprescindível a pronta atuação do poder judiciário para proibir uma prática manifestamente abusiva e indenizar os danos causados individual e coletivamente aos consumidores brasileiros e à sociedade brasileira, como um todo". A manipulação digital executada tem seu êxito enquanto o consumidor acredita que no âmbito virtual é possível ser livre e fazer escolhas, quando, na realidade, as empresas têm o controle, podendo algumas iludir com oferecimento de falsas ofertas, com preços diferenciados conforme o perfil do cliente.

As evidências foram colhidas quando oficiais notariais do Brasil e da Argentina efetuaram ao mesmo tempo operações e enquanto se comunicavam por telefone, para locar acomodações idênticas no dia 04 de maio de 2016. A intenção era "alinhar as buscas por hospedagem em horário idêntico[47]". Nesse mesmo dia as hospedagens para o Hotel Biarritz, o Villa Teresa Hotel e Hospedagem Ledo figuravam como indisponíveis para os brasileiros e disponíveis para argentinos. Em relação a outros hotéis[48], o valor das acomodações com as mesmas características, requeridas para o mesmo período, era mais alto para brasileiros do que para clientes de outras origens. Em outras palavras, os hotéis solicitavam cobrança de preços diversificada conforme a nacionalidade *do produto* (nesse caso, o consumidor sujeito de dados) e a empresa transmitia as ofertas.

Com a progressiva amplificação do *big data* a discriminação de consumidores oriunda de dados pessoais, principalmente quando são coletados e usados sem o conhecimento ou o consentimento informado do consumidor, são ameaças reais à neutralidade, autonomia e livre escolha na contratação de serviços. As probabilidades de expropriação de recursos financeiros tomando por base a 'fraqueza' dos consumidores cresce vertiginosamente.

A atitude da Decolar.com enseja o desequilíbrio das relações de consumo e vai de encontro ao determinado no Marco Civil da Internet em relação à neutralidade. Saliente-se que no Código de Defesa do Consumidor não há regras que caracterizem as práticas de *geo pricing* e *geo blocking*`, mas dispõe de cláusulas gerais e regras mais amplas capazes de identificar a ilicitude desses atos. Os direitos violados se referem a comportamentos contrários a equidade nas contratações, ao conhecimento e a proteção contra quaisquer abusos, a proibições singulares presentes no próprio Código, sendo elas o aumento sem

[47] MPRJ ajuíza ação inédita contra empresa de comércio eletrônico - Decolar.com. Ministério Público do Rio de Janeiro. 04 de fev. de 2018. atual. 02 de fev. 2018. Disponível em <http://www.mprj.mp.br/home/-/detalhe-noticia/visualizar/54503>. Acesso em: 22 de set. 2018.
[48] Sheraton Barra Rio de Janeiro Hotel, Windsor Oceânico e Linx Hotel International Airport.

justificativa do valor de produtos ou serviços ou recusar a venda destes diretamente a quem queira a adquiri-lo por meio de pronto pagamento.

Saliente-se que a Lei n° 12.529/2011 (lei antitruste) dispõe sobre a legitimidade de "dividir em partes ou segmentos um mercado atual ou potencial de bens e serviços por meio da distribuição de clientes, fornecedores, regiões ou serviços" (§ 3°, alínea c) e "discriminar adquirentes ou fornecedores de bens ou serviços por meio da fixação diferenciada de preços, ou de condições operacionais de venda ou prestação de serviços" (§3°, inciso X).

Assim, é necessário haver razoabilidade na motivação que trata consumidores de maneira desigual. Como o único "preceito" adotado pela Decolar.com foi a posição geográfica, é certo se depreender que tal atitude poderia ser facilmente enquadrada no rol de infrações da legislação antitruste, desde que haja "comprovação de sua posição dominante".

Segundo a lógica econômica, é possível atribuir preços maiores a produtos e serviços para consumidores dispostos a pagar mais. No entanto, quando há abuso com discriminação de clientes em condições equivalentes, considerando-se os dados pessoais quanto à sus posições no mapa, há danos à licitude do ato ante à racionalidade jurídica, no que tange à precificação realizada em "colaboração" com os hotéis interessados.

A ação movida pelo Ministério Público do Rio de Janeiro contra a empresa seguramente abriu precedentes (e os olhos!) contra as práticas de *geo blocking* e *geo pricing* mediante utilização indevida ou não consentida das informações digitais dos consumidores. Este posicionamento foi corroborado pela condenação ao pagamento de multa no valor de R$7.500.000,000 (sete milhões e quinhentos mil reais) a que foi submetida a Decolar, proferida pelo Departamento de Proteção e Defesa do Consumidor da Secretaria Nacional de Relações de Consumo do Ministério da Justiça.

CAPÍTULO 3 – PROTEÇÃO DE DADOS DOS USUÁRIOS NA U.E.: A GENERAL DATA PROTECTION REGULATION (OU REGULAMENTO GERAL DE PROTEÇÃO DE DADOS)

No âmbito internacional podemos citar o RGDP, norma proposta em 2012 e aprovado pela União Europeia em abril de 2016, em vigor desde 25 de maio de 2018. É um regulamento do Parlamento Europeu e do Conselho (EU 2016/679) que diz respeito à proteção, tratamento e livre circulação de dados de pessoas singulares, válido para todos os países membros da União Europeia e visa intensificar a aplicação da Proteção de Dados, constante na Carta dos Direitos Fundamentais da União Europeia, art. 8°. Afirma que a proteção de dados é direito fundamental que deve ser equilibrado com outros direitos fundamentais, não sendo a proteção um direito absoluto. Trouxe importantes contribuições à defesa do conteúdo privado dos indivíduos e é considerado parâmetro para os ordenamentos jurídicos regionais. Suas principais características são a seguir elencadas.

3.1. AUMENTO DA COMPETÊNCIA TERRITORIAL

A General Data Protection Regulation tem aplicabilidade extraterritorial: se destina aos casos em que as atividades de tratamento de dados sejam relativas a oferta de bens ou serviços a titulares de dados, independentemente de serem associadas a um pagamento. Neste caso o responsável pelo tratamento dos dados ou o subcontratante não precisa estar na União Europeia. Em outras palavras, as empresas responsáveis pelo processamento de dados de pessoas que residem na União Europeia podem ser responsabilizadas por qualquer ato que atente contra a vida privada das pessoas, podendo a empresa ser de qualquer parte do mundo, seja ela controladora ou processadora. As empresas que não fazem parte da União terão que nomear um representante que esteja na U.E.

3.2. DO CONSENTIMENTO

O artigo sexto disciplina que o consentimento é um requisito necessário, um fundamento, para a validade do processamento de dados pessoais para qualquer finalidade.

Conforme parágrafo trinta e dois do diploma o consentimento representa "...uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrônico, ou uma declaração oral".

Desta definição se entende que o silêncio, as omissões e opções pré-validadas não constituem, por si, uma autorização para o uso de dados. Como condições de validade há a clareza e a distinção de outros assuntos, além de ser fornecido de maneira compreensível e de fácil acesso. Assim, as empresas não podem usar termos e condições longos e ilegíveis.

O consentimento não é válido quando obtido de pessoas menores de dezesseis anos que deverão ser representadas, no ato, pelos seus responsáveis. Vale frisar que a idade pode ser especificada por cada país como forma de adaptação do Regulamento às necessidades sociais de cada nação.

3.3. DAS PENALIDADES

Quando uma organização comete infrações em relação ao regulamento, está sujeita a multas que podem chegar a 20 milhões de euros ou 4% do faturamento anual. Se trata da maior multa aplicada às infrações mais graves como a falta de consentimento do titular de dados para o processamento ou controle destes. Outra multa diz respeito à falta de ordem nos registros da empresa ou à falta de notificação da autoridade supervisora e do titular de dados quando ocorrer um vazamento. Acerca dessas infrações a organização responde com multa de dois por cento do faturamento total anual.

3.4. DOS DIREITOS DO SUJEITO DE DADOS PESSOAIS

Como um dos principais objetivos do RGPD é garantir a privacidade e a proteção de dados, foram criadas condições para que as pessoas exercessem esses direitos fundamentais. Dentre os indicados pelo regulamento há o direito à informação, segundo o qual o titular pode solicitar informações a organizações para saber quais dados pessoais seus estão sendo utilizados e o local e motivo para seu processamento, em formato estruturado e legível por máquina. Um cliente tem o direito de possibilitar a lista de processadores que acessam os dados.

O Regulamento também prevê o direito à portabilidade de dados que permite ao detentor destes solicitar ao responsável pelo tratamento a entrega das informações em formato estruturado e usual, que preze pela interoperabilidade, requerendo uma leitura automática dos dados com sua reutilização. Dessa forma, pode-se garantir o estímulo à livre circulação de conteúdos pessoais, facilitando a transferência entre distintos tomadores de serviços, desde que haja o consentimento do titular.

Quanto ao direito de acesso, o indivíduo detentor dos dados pode ter acesso a informações que circulam a seu respeito, bem como quais são trocados entre a empresa que processa esses dados pessoais e outras empresas parceiras. O titular pode ver seus próprios dados e solicitar cópias deles que o controlador[49] ou processador tem obrigação de fornecer.

Por fim, para a efetivação do direito ao esquecimento ou apagamento do conteúdo privado ou íntimo, o titular de dados pode determinar que o controlador apague os dados pessoais, interrompa a disseminação dos dados e, potencialmente, terceiros suspendam o processamento dos dados. Para que isso ocorra é necessário que os dados não sejam importantes para propósitos originais de processamento, ou seja, deixaram de ser importantes para a finalidade para a qual foram destinados. Outro motivo que consta no artigo 17 é o fato de os dados serem tratados de forma ilícita.

[49] Os controladores de dados (*data* controllers) definem o motivo do processamento de dados e a forma como as informações serão processadas de acordo com o objetivo a ser alcançado. Tomam decisões essenciais, ao contrário do processador, que possui poder decisório limitado. Segundo o RGPD, o controlador pode ser pessoa física ou jurídica, autoridade pública, agência ou outro órgão que, isoladamente ou em conjunto com outros, ocupam-se das informações pessoais. Os processadores (*data processors*) definem, dentro dos parâmetros estabelecidos pelo controlador, a organização dos dados coletados. A obtenção inicial do dado corresponde ao processamento e o resultado deste é o dado processado que é encaminhado ao usuário final. Conforme o regulamento, o encarregado de dados (*data protection officer*) é contratado pelo controlador e tem o dever de obedecer ao sigilo e confidencialidade quanto ao exercício de suas funções, que são descritas no artigo 39. Possuem a prerrogativa de desempenhar sua funções com independência.

CAPÍTULO 4 – LEGISLAÇÃO BRASILEIRA ACERCA DA PROTEÇÃO DE DADOS

Até recentemente o ordenamento jurídico brasileiro não dispunha de uma legislação específica para tratamento, transmissão e proteção de informações pessoais, principalmente as de caráter sensível. Como balizadores primordiais para regular as relações sociais, consumeristas, jurídicas ou negociais, dentre outras, eram utilizados os direitos fundamentais presentes na Constituição Federal e os direitos previstos no Código de Defesa do Consumidor, além da legislação regulatória de setores específicos. Destaquem-se os projetos legislativos e a alteração à Lei n°12.965/2014 como aperfeiçoamento do ordenamento jurídico quanto à tutela do conteúdo privado e íntimo do sujeito de dados. Segue, então, a breve citação das seguintes normas e projetos de lei que contribuíram para a origem da LPDP:

- Decreto n. 8.771, de 11 de maio de 2016, que regulamenta o Marco Civil da Internet. Esta norma trouxe regulamentação quanto "às hipóteses de rompimento da neutralidade da rede (art. 9º, §1º), as diretrizes de segurança e de sigilo dos dados pessoais (art. 10, §4º), o modo pelo qual os provedores de conexão e de aplicações deverão prestar informações sobre o cumprimento da legislação referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações (art. 11, §3º e 4º), a obrigação de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança (art. 13), a obrigação do provedor de aplicações de internet de manter os registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de seis meses, nos termos do regulamento (art. 15)[50]";
- Decreto n. 8.777, de 11 de maio de 2016, que institui a Política de Dados Abertos do Governo Federal, segundo o qual o principal gestor da política de dados abertos é o Ministério do Planejamento, através da Infraestrutura Nacional de Dados Abertos. Essa Política Nacional tem como objetivos fundamentais a promoção da transparência, o engajamento na participação social, o desenvolvimento de novos e melhores serviços governamentais e o aumento da integridade pública. O fomento tecnológico com o emprego de dados abertos é o pilar principal para o desenvolvimento de governos mais abertos, efetivos e responsáveis. – conforme o Portal Brasileiro de dados abertos. O decreto conceitua dados como sequência de símbolos ou valores,

[50] SANTOS, Coriolano Aurélio de Almeida Camargo; CRESPO, Marcelo. Neutralidade na Internet: a quem interessa o debate. Migalhas. 10 abr. 2015. Disponível em: <http://www.migalhas.com.br/DireitoDigital/105,MI218729,11049Neutralidade+da+internet+a+quem+interessa+o+debate> Acesso em: 28 jun. 2018.

representados em qualquer meio, produzidos como resultado de um processo natural ou artificial e dados abertos são os acessíveis ao público para livre utilização, consumo ou cruzamento. Os itinerários de transportes públicos utilizados por aplicativos são exemplo de dados abertos que trazem benefícios à sociedade;

- Projeto de Lei do Poder Executivo n. 5. 276/2016, que dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Este projeto foi aprovado pela Câmara dos Deputados em 28.05.2018. No entanto, foi arquivado em virtude da aprovação de outro projeto de lei, o de n. 4.060/2012;
- Projeto de Lei do Senado Federal n. 330/2013, que dispõe sobre a proteção, o tratamento e o uso dos dados pessoais que se encontra na Comissão de Assuntos Econômicos do Senado. Tratava da proteção, tratamento e utilização de dados das pessoas físicas e jurídicas de direito público ou privado. No que se refere à segurança pública, investigação criminal e instrução penal, administrativa e tributária são competentes órgãos públicos ou pessoas jurídicas de direito público. Dispunha que os procedimentos relativos a dados e informações sigilosas de interesse da segurança nacional fiquem a cargo de servidores públicos;
- Projeto de Lei da Câmara dos Deputados n. 4060/2012, que dispunha sobre o tratamento de dados pessoais, foi aprovado em 29.06.2018 quando foi desapensado do PL n. 5.276. Trata-se de um dos esboços da Lei de Proteção de Dados Pessoais e propunha a alteração do Marco Civil da Internet. Como princípios da proteção atinentes ao titular há o respeito à privacidade, à liberdade de informação, expressão, comunicação e opinião, à inviolabilidade da intimidade, honra e imagem. Em relação aos dados pessoais dispõe sobre as situações em que o tratamento é possível, sendo a primeira delas o consentimento do titular. Em agosto, este projeto foi convertido na atual Lei de Proteção de Dados Brasileira que entrará em vigor em fevereiro de 2020. A norma tem como principal veto a instituição da Agência Nacional de Proteção de Dados, cuja justificativa foi o vício de iniciativa do Poder Legislativo.

4.1. LEI NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS

As revelações feitas por Edward Snowden em 2013 acerca da espionagem da Agência Nacional de Segurança dos Estados Unidos em relação a executivos de empresas com

influência no mercado externo e autoridades nacionais e internacionais, inclusive a Presidente da República na época, Dilma Rousseff, abalaram as relações diplomáticas de vários países com os Estados Unidos (e se pode incluir o Brasil!). Apesar de o Marco Civil da Internet tratar da inviolabilidade e do sigilo das comunicações, não é suficiente para tratar de forma mais abrangente, e ao mesmo tempo específica, o tratamento e a proteção de dados pessoais.

Neste contexto, a missão das empresas se compõe em estruturar e efetuar uma ordem de critérios em modo de telas de aparecimento instantâneo (os denominados *pop ups*), com o objetivo de requerer a ciência do manuseio de dados, protocolos de confirmação e cadastros rápidos dos usuários em endereços eletrônicos, como também através dos *e-mails* de propaganda de empresas 'parceiras'. É requerido o consentimento dos clientes para que seus dados permaneçam disponíveis nos bancos de dados dessas empresas mesmo depois de concluídas as operações comerciais.

Sancionada em agosto, a Lei Geral de Proteção de Dados, claramente inspirada no Regulamento Geral de Proteção de Dados Europeu, tem a pretensão de fazer do sujeito de dados o principal responsável pelo consentimento para utilização de suas informações pessoais por terceiros, ou seja, há inversão do ônus a fim de que a pessoa possa dispor de suas informações. Os princípios básicos, então, seriam o consentimento do usuário, sujeito detentor dos dados, e a legitimidade do tomador dessas informações. É sobre estes que será construída a relação jurídica e sobre os quais haverá debates em caso de descumprimento legal ou impremeditação.

Nesse ponto, cite-se como exemplo, uma empresa que coleta os dados da saúde de seus funcionários para acompanhar os comportamentos a fim de melhorar a produtividade, incentivar a política de relacionamento e, possivelmente, dar folgas quando necessário, ou seja, um programa para melhorar a administração de riscos de uma instituição.

Se, porventura, a empresa compartilha esses dados sem consenso do empregado com algum plano de saúde, ocorre manipulação fraudulenta, pois, por um lado, há infração à livre concorrência, e por outro não houve consentimento do funcionário para a disseminação do conteúdo, em desrespeito aos princípios da transparência, proporcionalidade, razoabilidade e legitimidade da operação.

4.1.1. *Compliance*: a implementação da norma

Conforme disposição da Lei 13.709/2018, as empresas tomadoras de dados pessoaiscon são responsabilizadas pelo tratamento destes dados o que envolve, total ou parcialmente, as atividades relacionadas com a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (art. 5°, X).

Observa-se que a Lei conceitua os princípios orientadores do tratamento dos dados, como também aponta as hipóteses de sua aplicação, incluindo os direitos dos titulares dos dados, o conceito das atribuições dos encarregados pela tomada das informações e a figura da autoridade nacional para proteção de dados, a ser definida por ato de iniciativa do Executivo.

Para garantir uma boa gestão de qualidade no tratamento, transmissão e armazenamento de dados as empresas terão que se adequar à nova norma desenvolvendo processos e procedimentos para acolher as queixas dos sujeitos de dados, respondendo-as, prestar esclarecimentos e adotar providências, construir a comunicação com a autoridade nacional, orientar os seus funcionários a respeito das práticas a serem tomadas em relação à proteção de dados pessoais, executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares (art. 41).

Dessa forma, a otimização dos fluxos das operações comerciais e dos recursos operacionais auxiliam na redução de gastos e as empresas que melhor se adequarem quanto à implementação dos requisitos legais, desviando-se ao máximo de inconvenientes regulatórios, além de ser vistas com bons olhos pelos potenciais consumidores, contribuem para a formação de um mercado mais ético.

Para tanto, organizações e empresas terão de aperfeiçoar suas metodologias institucionais para garantir a segurança de dados cadastrais e dados sensíveis condizente aos seus fornecedores e clientes. Nesse aspecto, organizações públicas e privadas necessitam do consentimento expresso do titular de dados para disponibilizá-los em bancos de dados ou compartilhá-los com outras entidades. A empresa ou organização deverá observar a clareza na solicitação com vistas a informar o cidadão sobre quais dados serão coletados, o motivo de sua coleta, se serão compartilhados e quem são os interessados nesses dados. O controlador terá obrigação de informar, também, a alteração de finalidade quanto ao compartilhamento de informações com terceiros a fim de que o usuário tenha a oportunidade de aceitar ou não a

nova situação. Ademais, o controlador deve atender aos pedidos de revogação de autorização, bem como conceder acesso, exclusão, complementação de dados, correção ou portabilidade.

A LPDP *teoricamente* confere ao Brasil protagonismo no que diz respeito à legislação de segurança de dados, sendo primordial para a inclusão do país nos foros internacionais, convergindo com legislações estrangeiras, além de promover um ambiente seguro para negócios capazes de atrair e materializar investimentos.

4.2. CÓDIGO DE DEFESA DO CONSUMIDOR: ALGUNS PRINCÍPIOS FUNDAMENTAIS QUE REGEM A PROTEÇÃO DOS DADOS

Uma importante balizadora das relações consumeristas, a Lei 8.078/1990 também tem em seus princípios fundantes, detentores de alta carga valorativa e avançado grau de subjetividade, o arcabouço necessário para se construir as regras orientadoras para a guarita do conteúdo pessoal particular.

A diferença central entre princípios e regras consiste na amplitude de seu alcance pedagógico: enquanto as regras requerem o cumprimento de normas, observando-se se estas se aplicam ao caso concreto ou não, os princípios requerem a adequação do fato à norma, conforme a possibilidade jurídica de sua aplicação. Assim, "segundo DWORKIN, enquanto as regras impõem resultados, os princípios atuam na orientação do sentido de uma decisão. Quando se chega a um resultado contrário ao apontado pela regra é porque ela foi mudada ou abandonada; já os princípios, ainda que não prevaleçam, sobrevivem intactos[51]". Assim, a abordagem de cláusulas gerais confere ao CDC caráter principiológico.

Constante no art. 1° da Lei Protetiva, o *Princípio da Proteção ao Consumidor* tem o objetivo de tutelar o consumidor sujeito de dados contra o desequilíbrio econômico entre este e o fornecedor de bens e serviços nas relações desenvolvidas nos meios físicos e eletrônicos. A integridade física, psíquica e econômica do consumidor são objeto de Ações Civis Públicas sempre que haja dano material e moral aos interesses difusos e coletivos, atribuindo legitimidade de atuação ao Ministério Público. Tome-se como exemplos os casos supramencionados nos quais a violação de dados de milhões de usuários interessa à sociedade em geral. Ademais, cabe ao Estado a defesa do consumidor como garantia à

[51] NOVELINO, Marcelo. *Direito Constitucional.* 9. ed. São Paulo: Método, 2014. p. 150.

existência digna, um dos fundamentos da ordem econômica, conforme art. 170 do Diploma Constitucional.

Mas, a proteção ao consumidor tem a colaboração do *Princípio da Precaução*, relacionado ao desconhecimento do consumidor quanto aos riscos presentes nos bens e serviços adquiridos. Para impedir prejuízos de difícil reparação à saúde ou segurança, de maneira geral, os fornecedores dos bens jurídicos devem fazer estudos de viabilidade de guarda e compartilhamento de dados e adotar técnicas para que, por exemplo, os dados do *vulnerável negocial* permaneçam sob sigilo. Diverge do *Princípio da Prevenção* que requer a proteção do consumidor contra riscos conhecidos como os sofridos quando seus dados são expostos, pondo em risco a privacidade financeira, social e econômica. A Lei 13.709/2018 orienta o fornecedor de serviços a adotar medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (art. 6°, VIII).

Para que as relações entre titular e tomador de dados se desenvolvam de forma salutar o *Princípio da Boa-fé Objetiva* foi o mérito utilizado pelo legislador na cadência de interesses de fornecedores e consumidores para facilitar a probidade e equidade na realização das atividades consumeristas. Este fundamento, presente no art. 4°, inciso III, da Lei Consumerista apresenta três funções: servir como fonte de novos deveres especiais de conduta durante o vínculo contratual, os denominados deveres anexos (*função criadora*), construir uma causa limitadora do exercício, antes ilícito, hoje abusivo, dos direitos subjetivos (*função limitadora*) e ser utilizada como concreção e interpretação dos contratos (*função interpretadora*)[52]. Como se observa na redação do art. 6° da LPDP, a boa-fé objetiva foi recepcionada como princípio basilar das atividades de tratamento de dados pessoais, em congruência com o Código de Defesa do Consumidor.

O princípio anterior é basilar do consentimento dado pelo consumidor titular de informações pessoais quando do fornecimento destes ao responsável pela guarda, armazenamento e tratamento. Para tanto, é necessária a aplicação do *Princípio da Transparência*, que no legado consumerista se encontra no *caput* do art. 4°, segundo o qual o respeito à dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a *transparência* e harmonia das relações de consumo são elementos fundantes do atendimento às necessidades dos consumidores.

[52] TARTUCE, Flávio; NEVES, Daniel Amorim Assumpção, 2017. p. 41 *apud* MARQUES, Claudia Lima; BENJAMIM, Herman; MIRAGEM, Bruno, 2010. p. 125.

O consumidor tem o direito de acesso à informação clara para formar sua convicção acerca das características dos produtos e serviços, resguardando a tutela das relações de consumo. Trata-se do *Princípio da Transparência* relacionado com a *proteção contra publicidade enganosa e abusiva*. Note-se que a transparência, prevista também como princípio necessário à tutela de dados, coaduna-se com o fundamento da segurança de conteúdo privativo e íntimo, segundo o qual os agentes de tratamento devem se valer de "de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão" (art. 6°, VII, LPDP).

Outro princípio pertinente às consequências advindas da falta de observância daqueles supramencionados diz respeito à *compensação integral do dano* ou *restitutio in integrum* que se perfaz nas efetivas prevenção e reparação de todos os danos suportados, sejam eles materiais ou morais, individuais, coletivos ou difusos[53] e engloba os juros cessantes. Seu objetivo é restituir ao consumidor o estado de equilíbrio anterior ao ato ilícito causador do dano por meio da efetivação de sanções postas ao fornecedor. Este princípio foi introduzido implicitamente no Diploma de Proteção de Dados conforme se depreende da redação do art. 52, *in verbis*:

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
>
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
>
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
>
> III - multa diária, observado o limite total a que se refere o inciso II;
>
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
>
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
>
> VI - eliminação dos dados pessoais a que se refere a infração;
>
> VII - (VETADO);

[53] TARTUCE, 2018. p. 62.

VIII - (VETADO)[54];

IX - (VETADO).

Conforme se vê os princípios que regem o Código de Defesa do Consumidor podem ser trasladados para a devida implementação da Lei de Proteção de Dados Pessoais.

5. CONVERGÊNCIA ENTRE BRASIL E UNIÃO EUROPEIA

As empresas e organizações pioneiras na implementação da legislação europeia sobre proteção de dados têm em vista a confiabilidade do consumidor na forma como o dado é manipulado. Como consequência, não sentirá maiores dificuldades em aplicar os princípios da Lei Geral de Proteção de Dados, pois têm os mesmos pilares que compensam os interesses de tomadores de dados pessoais, controladores e encarregados dentro das empresas.

A convergência entre legislações é fundamental para uma interação mais efetiva entre países de modo que o compartilhamento de dados é facilitado. Os princípios basilares, inerentes à regulação das informações pessoais, que devem nortear as relações entre instituições públicas, privadas e de titulares de dados, abarcam os pontos fulcrais da diversidade legislativa dentro de uma comunidade, podendo ser flexíveis quanto à sua interpretação, quando exigido pelas circunstâncias.

Neste contexto, deve-se observar, como elementos formadores da legislação a sua abrangência em relação aos mais diversos setores sociais e econômicos, (a) a combinação de diversas estruturas legais, (b) a presença de uma autoridade nacional de proteção de dados, (c) sistema de responsabilização de autoridades públicas ou privadas (*accountability*), (d) o controle dos próprios dados pelo seu legítimo detentor, ou seja, aquele que tem o poder de gerar informações que interessam a terceiros, (e) o elo adstrito entre a observância das regras de privacidade e a diligência da autoridade voltada à matéria de dados.

A convergência entre normas e sua implementação é necessária para tornar congruentes, o máximo possível, os processos e procedimentos de setores diferentes. A neutralidade da estrutura legal converge para a funcionalidade e circulação dos dados, algo que propicia um ambiente mais harmônico nas relações entre titulares de dados e os setores

[54] Os incisos VII, VIII e IX tratavam das sanções administrativas quando houvesse violação das previsões legais. Dispunham sobre a suspensão parcial ou total de atividades voltadas ao tratamento de dados, bem como do funcionamento de bancos de dados ligados à violação. Dessa forma, o órgão responsável pela fiscalização e aplicação da norma perde muito seu caráter sancionatório.

públicos e privados. Por esse motivo, tanto o Regulamento Europeu como a LPDP prezam pela abrangência legislativa a fim de adequar diferenças regulatórias.

Também, é possível ver a importância do papel da Autoridade Nacional de Proteção de Dados quanto à fiscalização do cumprimento das normas e a intermediação ente usuários e tomadores, controladores e encarregados de dados. A Autoridade Nacional é responsável por vindicar o comportamento adequado das empresas e organizações quanto ao estabelecimento de rotinas voltadas à segurança das informações e seu compartilhamento com terceiros.

CONCLUSÃO

É incontroverso que desde o surgimento do primeiro computador, o *Electrical Numerical Integrator and Calculator* (ENIAC), a velocidade das transformações sentidas pela sociedade é surpreendente.

Não existem fatos preexistentes tão significativos quanto a progressão das formas de comunicação humana por mídias digitais. Ações como comer, comprar ou vender mercadorias e serviços, publicar propagandas, pedir um transporte, fazer movimentações financeiras, relacionar-se são facilitadas por aplicativos disponíveis à mão. As informações são concebidas instantaneamente e aqueles que não introduzem a tecnologia e inovação ao seu cotidiano ficam desatualizados e à parte do contexto social. Mas, para se ter acesso aos produtos e serviços o indivíduo tem de efetuar o cadastro prévio de seus dados. Como saber se eles estão seguros?

Conforme disposto anteriormente, o ordenamento pátrio não dispunha de regulamentação específica até a sanção da Lei nº 13.709/2018. A proteção à privacidade de dados pessoais tinha, e ainda tem, por base o artigo 5º, inciso X da Constituição Federal, sendo, posteriormente, associado ao artigo 8º da Lei nº 12.965/2014, o Marco Civil da Internet, norma setorial relativa aos serviços de Internet que abrange, tão somente, a proteção às informações pessoais naquela esfera.

Em relação à convergência, necessária para livre circulação de dados, ressaltam-se a importância do consentimento na relação entre consumidores titulares de dados e responsáveis pelo tratamento, o dever de zelar pela transparência e segurança, os direitos quanto ao acesso, retificação, cancelamento ou apagamento de dados e o sigilo das informações pessoais. Esses pontos são predominantes no Regulamento europeu e na LPDP e servem de lastro para a

função fiscalizadora do Estado que, na União Europeia, está presente na Autoridade Europeia para a proteção de dados.

Mas, não obstante a criação e implementação de leis específicas sobre proteção de conteúdos pessoais privados, a sociedade se depara com controvérsias quanto ao tratamento de dados pessoais e escândalos que envolvem vazamentos ou utilização adversa das informações sem consentimento do usuário. Esse fato representa sinal de alerta quando o controle compartilhado de dados com terceiros se presta à manipulação de pensamentos para diversos fins e vêm o indivíduo como mero ente mercadológico. Por esse motivo a proteção à privacidade individual e social é indispensável para o exercício das liberdades fundamentais.

Entretanto, a produção legislativa regional ainda não é capaz de atingir a complexidade dos algoritmos e, tampouco, a velocidade com que novas tecnologias são desenvolvidos e postas em circulação no mercado digital de dados. Dessa forma, é certo dizer que não existe uma solução específica ou um modelo capaz de atender as diversas demandas, haja vista a necessidade cultural divergente de uma sociedade para outra e que a projeção de um sistema particular de dados deve ser adequada a condições econômicas e políticas e a tradições jurídicas.

Nesse contexto, como forma de resguardar o máximo possível a privacidade e o mercado digital de dados, é fundamental a amplificação da legislação local para que seja possível a interação entre setores sociais distintos. Mudar é preciso. E estar de olhos abertos, também!

REFERÊNCIAS BIBLIOGRÁFICAS:

OBRAS:

ALEXY, Robert. *Teoria de los derechos fundamentales*. Madrid: Centro de Estudios Constitucionales, 1993.

CRISTÓVAM, José Sérgio da Silva. A resolução das colisões entre princípios constitucionais, 2010.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. 448 p.

FILHO, Eduardo Tomasevicius. Em direção a um novo 1984? A tutela da vida privada entre a invasão de privacidade e a privacidade renunciada Revista da Faculdade de Direito da Universidade de São Paulo, v.109, p. 129-169, 2014.

HUBMANN, Heinrich. Das Persönlichkeitsrecht. Böhlnau – Verlag Münster / Köln, 1967.

MENDES, Gilmar Ferreira. Direitos Fundamentais e controle de Constitucionalidade. São Paulo: Saraiva, 2004.

MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. Curso de Direito Constitucional. São Paulo: Saraiva, 2009. p 172.

MIRANDA, Leandro Alvarenga. A proteção de dados pessoais e o paradigma da privacidade. São Paulo: All Print Editora, 2018.

MORAIS, Alexandre de. Curso de Direito Constitucional. 14 ed. São Paulo: Atlas, 2003.

NOVELINO, Marcelo. Manual de direito constitucional. São Paulo: Editora Método, 2014.

PAESANI, Liliana Minardi. Direito e Internet: liberdade de informação, privacidade e responsabilidade civil. São Paulo: Atlas, 2000.

PINHEIRO, Patrícia Peck (organização). *et al*. Direito digital aplicado 3.0. 1.ed. São Paulo: Thompson Reuters Brasil, 2018.

SALDANHA, Nuno. Novo Regulamento Geral de Proteção de dados: o que é? A quem se aplica? Como implementar? São Paulo: FCA, 2018.

SARMENTO, Daniel. GALDINO, Flávio. Direitos Fundamentais: estudos em homenagem ao professor Ricardo Lobo Torres. Rio de Janeiro: Renovar, 2006.

SCHERTEL, Laura Mendes. Privacidade, proteção de dados pessoais e defesa do consumidor: linhas gerais de um novo direito fundamental. Série IDP. São Paulo: ed. Saraiva, 2014.

SHU, Xiaokui. *et al*. *Breaking the Target: An Analysis of Target Data Breach and Lessons Learned*. Cornell University Library. 18 jan. 2017.

SZANIAWSKI, Elimar. Direitos de personalidade e sua tutela. 2.ed. São Paulo: Editora Revista dos Tribunais, 2005.

TARTUCE, Flávio; NEVES, Daniel Amorim Assumpção. Manual de Direito do Consumidor: direito material e processual. 6. ed. rev. atual. e ampl. Rio de Janeiro: Forense; São Paulo: MÉTODO, 2017.

UNIÃO EUROPEIA: Tribunal de Justiça da União Europeia. Conclusões do advogado geral Niilo Jääskinen, 25 de junho de 2013, 2013. Disponível em: http://curia.europa.eu/juris/document/document_print.jsf?doclang=PT&text=&pag eIndex=0&part=1&mode=req&docid=138782&occ=first&dir=&cid=1006183. Acessado em 28 jun. 2018.

ENDEREÇOS ELETRÔNICOS CONSULTADOS:

AIGRAIN, Philippe. *L'individu et la société à l'age numérique: entre capture et emancipation*. O indivíduo e a sociedade na era digital: entre captura e emancipação, palestra dada no Sindicato da Magistratura, 20-21 de setembro de 2014, Lille, Disponível em: http://paigrain.debatpublic.net/?p=8944. Acessado em 28.06.2018.

BRASIL. Senado Federal. Parecer quanto aos Projetos de lei n°330/2013, 131/2014 e 181/2014. p.4 *apud http://www.refworld.org/docid/453883f922.html*. Disponível em <file:///C:/Users/CL%20PC/Downloads/DOC-Relat%C3%B3rio%20Legislativo%20-%20SF175648629127-20171003%20(1).pdf> Acesso em: 08 de set. 2018.

COELHO, Gabriela. MP-DF pede a condenação de banco por vazamento de dados pessoais de clientes. São Paulo, 31 jul. 2018. Disponível em: < https://www.conjur.com.br/2018-jul-31/mp-df-condenacao-banco-vazamento-dados-pessoais> Acesso em: 22 set. 2018.

EL PAÍS. O marqueteiro brasileiro que importou o método da campanha de Trump para usar em 2018. El País. São Paulo. 15 out. 2017. Disponível em: <https://brasil.elpais.com/brasil/2017/10/11/politica/1507723607_646140.html> Acesso em: 09 nov. 2018.

FERRAZ JR, Tércio Sampaio. Sigilo de dados: o Direito à privacidade e os limites à função fiscalizadora do Estado, 2011. Disponível em.: < http://www.terciosampaioferrazjr.com.br/?q=/publicacoes-cientificas/28>. Acesso em: 08 set. de 2018

GANJOO, Shweta. Facebook multado em Rs 4 crore no Reino Unido por seu papel no escândalo Cambridge Analytica. India Today. Nova Delhi, 11 jul. 2018. Disponível em < https://www.indiatoday.in/technology/news/story/facebook-fined-over-rs-4-crore-in-uk-for-its-role-in-cambridge-analytica-scandal-1282509-2018-07-11> Acesso em 10 out. 2018.

HALPIN, Padraic. *Facebook's lead EU regulator opens probe into data breach*. *Cyber Risk.* Reuters.03 out. 2018. Disponível em: <https://www.reuters.com/article/us-facebook-cyber-ireland/facebooks-lead-eu-regulator-opens-probe-into-data-breach-idUSKCN1MD2EC> Acesso em: 10 out. 2018.

MINISTÉRIO PÚBLICO DO RIO DE JANEIRO. MPRJ ajuíza ação inédita contra empresa de comércio eletrônico - Decolar.com. 04 fev. 2018. Disponível em: <http://www.mprj.mp.br/home/-/detalhe-noticia/visualizar/54503>. Acesso em: 22 de set. 2018.

NICBR VÍDEOS. IX Seminário sobre privacidade e proteção de dados pessoais. São Paulo, 2018. Disponível em: < https://www.youtube.com/watch?v=SRtDI7uCb8M&t=12963s> Acesso em: 22 ago. 2018.

NOVELLI, Heitor Bueno. A proteção de dados no Brasil e na Europa: um comparativo entre a legislação brasileira e o modelo europeu. Trabalho de conclusão de curso apresentado ao Curso de Graduação em Direito, Setor de Ciências Jurídicas da Universidade Federal do Paraná. 2017. Disponível em https://www.acervodigital.ufpr.br/bitstream/handle/1884/55929/HEITOR%20BUENO%20NOVELLI.pdf?sequence=1.

OLHAR DIGITAL. Jovem move processo contra o Facebook por guardar seus dados na rede, 2011. Disponível em <https://olhardigital.com.br/noticia/facebook-tera-de-pagar-r245-mil-por-guardar-dados-que-foram-deletados/22681> Acesso em: 12 nov. 2018.

PAYÃO, Felipe. Banco Inter é extorquido e dados de clientes são expostos. TecMundo. 04 mai. 2018. Disponível em: <https://www.tecmundo.com.br/seguranca/129811-exclusivo-vazam-dados-400-mil-clientes-banco-inter.htm> Acesso em: 08 set. 2018.

REGANIN, Paulo. Lei Geral de Proteção de Dados – Análise. LEGAGE. 17 ago. 2018. Disponível em: <https://vazdealmeida.com/lei-geral-de-protecao-de-dados-pessoais-%E2%80%95-analise/> Acesso em: 09 nov. 2018.

ROMM, Tony; Dwoskin, Elizabeth. Facebook is slapped with first fine for Cambridge Analytica scandal. The Washington Post. Business. 10 jul. 2018. Disponível em: <https://www.washingtonpost.com/business/economy/2018/07/10/5c63a730-848b-11e8-8f6c-46cb43e3f306_story.html?utm_term=.3d0734750f6e> Acesso em: 10 out. 2018.

SANTOS, Coriolano Aurélio de Almeida Camargo; CRESPO, Marcelo. Neutralidade na Internet: a quem interessa o debate. Migalhas. 10 abr. 2015. Disponível em: <http://www.migalhas.com.br/DireitoDigital/105,MI218729,11049Neutralidade+da+internet+a+quem+interessa+o+debate> Acesso em: 28 jun. 2018.

SERAFINO, Ana Teresa. Direito à Portabilidade dos Dados Pessoais: um novo direito dos titulares dos dados e um novo desafio para os responsáveis pelo tratamento. IT Channel. Portugal, 01 abr. 2017. Disponível em: http://www.plmj.com/xms/files/2017_PDF/Portabilidade_Dados_Pessoais_Ana_Teresa_Serafino.pdf> Acesso em: 12 out. 2018.

SERRATO, Jeewon Kim. *et al.* Estados dos EUA aprovam leis de proteção de dados logo após a GDPR. *Compliance and risk*. 09 jul. 2018. Disponível em <https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/>. Acesso em 20 set. 2018.

SILICONANGLE. Facebook pode ser multado em até US$ 1,63 bilhão pela última violação de dados. Atualizado em 30 set. 2018. Disponível em: <https://siliconangle.com/2018/09/30/facebook-face-fine-upto-1-63b-eu-latest-data-breach/> Acesso em: 10 out. 2018.

THOREN-PEDEN, Deborah. MAYER, Catherine. *Data Protection 2018 – laws and regulations. International Comparative Legal Guides*. 12 jun. 2018. Disponível em: < https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa> Acesso em: 20 set. 2018.

LEGISLAÇÃO E JURISPRUDÊNCIA CONSULTADAS

ALEMANHA. *Land de Hesse.* Hessisches Datenschutzgesetz (HDSG). Disponível em: <https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/content-downloads/HDSG.pdf> Acesso em 08 set. 2018.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil: promulgada em 5 de outubro de 1988. Organização do texto: Juarez de Oliveira. 4. ed. São Paulo: Saraiva, 1990. 168 p. (Série Legislação Brasileira).

_____. Lei n. 10.406, de 10 de janeiro de 2002. Código Civil.

_____. Lei n. 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor.

_____. Superior Tribunal de Justiça. REsp n° 1.749.804, Relator Ministro Antonio Carlos Ferreira, DJ 25/09/2018.

_____. Superior Tribunal de Justiça. REsp n° 1.348.532 SP 2012/0210805-4, Relator Ministro Luís Felipe Salomão, DJ 30/11/2017.

CALIFORNIA LEGISLATIVE INFORMATION. *Legislative Counsel's Digest. The California Consumer Privacy Act of 2018.* Disponível em <https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375&search_keywords=California+Consumer+Privacy+Act+of+2018> Acesso em: 21 set. 2018.

COGAN, Marin. *Cambridge Analytica Whistleblower Brittany Kaiser Is Out to Clear Her Name*. 2018. Disponível em: < https://www.elle.com/culture/tech/a21272094/brittany-kaiser-cambridge-analytica-interview/> Acesso em: 12 set. 2018.

Conselho da Europa. Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal. Estrasburgo – França, 1081.

CONSELHO DA OCDE. Organização para a Cooperação e Desenvolvimento Econômicos. Diretrizes sobre a Proteção da Privacidade e Fluxos Tranfronteiriços de Dados, 1980.

COUNCIL OF EUROPE. *European Court of Human Rights. European Convention for the Protection of Human Rights and Fundamental Freedoms*. Strasboug, 1950. Disponível em: <https://www.echr.coe.int/Documents/Convention_POR.pdf>. Acesso em: 09 set. 2018.

ESTADOS UNIDOS. Federal Trade Commission (FTC) – Protecting America's Consumers. *Facebook settles FTC charges that it deceived consumers by failing keep privacy promisses*. 2011.

_____. Congresso dos Estados Unidos da América. HR4943. 115° Congresso do Cloud Act (2017-2018).

_____. Senado. *Constitution of the United States*. *Amendment IV*. 1791. Disponível em: <https://www.senate.gov/civics/constitution_item/constitution.htm#amdt_4_1791> Acesso em: 09 set. 2018.

LOUISIANA STATE LEGISLATURE. *Database Security Breach Notification Law – Act n° 382*. Louisiana, 2018. Disponível em <https://www.legis.la.gov/legis/ViewDocument.aspx?d=1101149>. Acesso em: 09 set. 2018.

Organização das Nações Unidas (ONU). Diretrizes para Regulamentação de arquivos de dados pessoais informatizados, em tradução livre. ONU – Organização das Nações Unidas. Disponível em <http://www.refworld.org/docid/3ddcafaac.html> Acesso em: 22 set. 2018.

Organization American States (OAS). *Privacy and Personal Data in the America*. CJI/Res. 186/2012 e CJI/Res. 212/2015. Disponível em <https://www.oas.org/en/sla/iajc/docs/ijc_current_agenda_privacy_personal_data_protection.pdf> Acesso em: 10 set. 2018.

_____. *El Comité Jurídico Interamericano adopta por consenso informe sobre Protección de Datos Personales.*2015. Disponível em <http://www.oas.org/es/sla/ddi/boletines_informativos_Proteccion_datos_personales_CJI_informe_Abr-2015.html> Acesso em: 10 set. 2018.

THE IOWA LEGISLATURE. *Relating to Student Personal Information Protection Act*. Iowa, 2018. Disponível em: < https://www.legis.iowa.gov/legislation/BillBook?ba=HF2354&ga=87> Acesso em: 09 set. 2018.

União Europeia. Parlamento Europeu e Conselho da União Europeia. Diretiva 2016/680, de 27 abr. 2016. Jornal Oficial da União Europeia. Bruxelas/BZ. 2016.

_____. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 abr. 2016. Jornal Oficial da União Europeia. Bruxelas/BZ. 2016.

ANEXOS

ANEXO 1 – ÍNDICE DE VIOLAÇÃO DE DADOS[55]

Organização violada	Registros violados	Data de Violação	Tipo de violação	Fonte de Violação	Localização	Indústria	Pontuação de risco
Facebook	2.200.000.000	04/04/2018	Roubo de identidade	Estranho Malicioso	Estados Unidos	Mídia social	***10***
Equifax	147.900.000	15/07/2017	Roubo de identidade	Estranho Malicioso	Estados Unidos	Financeiro	***10***
Reliance Jio	120.000.000	07/10/2017	Acesso à conta	Estranho Malicioso	Índia	Tecnologia	***10***
Friend Finder Networks	412,214,295	16/10/2016	Dados Existenciais	Estranho Malicioso	Estados Unidos	Entretenimento	***10***
Anthem Insurance Companies (Anthem Blue Cross)	78.800.000	27/01/2015	Roubo de identidade	Estado Patrocinado	Estados Unidos	Cuidados de saúde	***10***
Yahoo	500.000.000	12/01/2014	Acesso à conta	Estado Patrocinado	Estados Unidos	Tecnologia	***10***
Home Depot	109.000.000	09/02/2014	Acesso Financeiro	Estranho Malicioso	Estados Unidos	Varejo	***10***
JPMorgan Chase	83.000.000	27/08/2014	Roubo de identidade	Estranho Malicioso	Estados Unidos	Financeiro	***10***
CyberVor	1.200.000.000	08/05/2014	Acesso à conta	Estranho Malicioso	Global	Tecnologia	***10***
eBay	145.000.000	21/05/2014	Roubo de identidade	Estranho Malicioso	Estados Unidos	Varejo	***10***
Korea Credit Bureau, NH Nonghyup Card, Lotte Card, KB Kookmin Card	104.000.000	20/01/2014	Roubo de identidade	Insider Malicioso	Coreia do Sul	Financeiro	***10***
Target	110.000.000	11/04/2013	Acesso Financeiro	Estranho Malicioso	Estados Unidos	Varejo	***10***
Adobe Systems, Inc	152.000.000	18/09/2013	Acesso Financeiro	Estranho Malicioso	Estados Unidos	Tecnologia	***10***

[55] Breach Level Index. Disponível em: <https://breachlevelindex.com/data-breach-database> Acesso em: 13 nov. 2018. Obs.: os índices variam cotidianamente.

Organização violada	Registros violados	Data de Violação	Tipo de violação	Fonte de Violação	Localização	Indústria	Pontuação de risco
Yahoo	1.000.000.000	08/09/2013	Roubo de identidade	Estranho Malicioso	Estados Unidos	Tecnologia	***10***
MySpace	360.000.000	11/06/2013	Acesso à conta	Estranho Malicioso	Estados Unidos	De outros	***10***
Motor Vehicles Department in Kerala	200.000.000	01/05/2017	Incômodo	Estranho Malicioso	Índia	Governo	***9,9***
General Directorate of Population and Citizenship Affairs, the General Directorate of Land Registry and Cadaster	50.000.000	01/12/2015	Roubo de identidade	Estranho Malicioso	Peru	Governo	***9,9***
Country's Supreme Election Committee (YSK)	54.000.000	16/12/2013	Roubo de identidade	Estranho Malicioso	Peru	Governo	***9,9***
iMesh	51.000.000	22/09/2013	Roubo de identidade	Estranho Malicioso	Estados Unidos	Tecnologia	***9,9***
River City Media	1.340.000.000	03/06/2017	Incômodo	Perda acidental	Estados Unidos	De outros	***9,8***

ANEXO 2 – CERTIFICADO DIGITAL E CHAVE PRIVADA DO BANCO INTER[56]


```
-----BEGIN CERTIFICATE-----
MIIFgjCCBGqgAwIBAgIJAJOP6jRxq1aHMA0GCSqGSIb3DQEBCwUAMIG0MQswCQYD
VQQGEwJVUzEQMA4GA1UECBMHQXJpem9uYTETMBEGA1UEBxMKU2NvdHRzZGFsZTEa
MBgGA1UEChMRR29EYWRkeS5jb20sIEluYy4xLTArBgNVBAsTJGh0dHA6Ly9jZXJ0
cy5nb2RhZGR5LmNvbS9yZXBvc2l0b3J5LzEzMDEGA1UEAxMqR28gRGFkZHkgU2Vj
dXJlIENlcnRpZmljYXRlIEF1dGhvcml0eSAtIEcyMB4XDTE3MDgxODE0MTAwM1oX
DTE5MDgxODE0MTAwM1owejELMAkGA1UEBhMCQlIxFTATBgNVBAgTDE1pbmFzIEdl
cmFpczEXMBUGA1UEBxMOQkVMTyBIT1JJWk9OVEUxHTAbBgNVBAoTFEJBTkNPIElO
VEVSTUVESVVNIFNBMRwwGgYDVQQDDBMqLmJhbmNvaW50ZXIuY29tLmJyMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAjqyIVcWrRePrQzJtqyV6LDWGHFdz
R2NfCnKND/C89iNld1Cx8XHdgGFZP/i17dAAwTH7NOC46OzQE0hh6sQVDqYW9ASz
7zEhD6Ey8WcXet2fKbyRDSyCKw1PTBNaZuIIlsaJjYTyWM135Ne6U8pYDWzK8XEj
hXF0kL4HB0Ctz6wAV+2jU+qm6mtBBC19+pGshi6cYENxwVSlmEAjc7a2gJnhfbQ/
vaH9o69DpLIm8Qie5/9Op/eSXn6E3dEmmSuw384abxmx4l0YEVTCs565kyFe0uEo
7tpHpkw7gDjnOOd6zV9cUCRyngbnTt8d+rDw0xo+sb7PWRZKur9ir/0hLwIDAQAB
o4IBzjCCAcowDAYDVR0TAQH/BAIwADApBgNVHSUEIjAgBggrBgEFBQcDAQYIKwYB
BQUHAwIGCmCGSAGG+E0BAgMwDgYDVR0PAQH/BAQDAgWgMDUGA1UdHwQuMCwwKqAo
oCaGJGh0dHA6Ly9jcmwuZ29kYWRkeS5jb20vZ2RpZzJzMi02LmNybDBdBgNVHSAE
VjBUMEgGC2CGSAGG/W0BBxcCMDkwNwYIKwYBBQUHAgEWK2h0dHA6Ly9jZXJ0aWZp
Y2F0ZXMuZ29kYWRkeS5jb20vcmVwb3NpdG9yeS8wCAYGZ4EMAQICMHYGCCsGAQUF
BwEBBGowaDAkBggrBgEFBQcwAYYYaHR0cDovL29jc3AuZ29kYWRkeS5jb20vMEAG
CCsGAQUFBzAChjRodHRwOi8vY2VydGlmaWNhdGVzLmdvZGFkZHkuY29tL3JlcG9z
aXRvcnkvZ2RpZzIuY3J0MB8GA1UdIwQYMBaAFEDCvSeOzDSDMKIz1/tss/C0LIDO
MDEGA1UdEQQqMCiCEyouYmFuY29pbnRlci5jb20uYnKCEWJhbmNvaW50ZXIuY29t
LmJyMB0GA1UdDgQWBBSHzZeDKoQUhspUMrTHeW3EFT40rDANBgkqhkiG9w0BAQsF
AAOCAQEAgPxW2bMBbZ2uctFnhKKlJh7S9ECJzZ2FVhZ1PAPYd54DZzqsjfLX5ntA
FK64dyau4/WkSGzMsJq/SkpuK17YKNKS0dLpujOTmcqEfqTrHVSbVKjClZfgDxit
DpkR9oEe9UzWrSyUFSTiDTr0Koibga4Uzgswf5RwajcSOD8BTgpfzJDO34ZOrdLu
Uk/MDq0689oWlWPYZwensoFS+R7kll3h9NLm19tsPkufL4rnnoFsmQxg1AZH3Wy9
itl7UReNrqXIqyc+rVKhEITddVZt/4RzVoTKMnRnpBW8rej95jm1VKYt80a3/JCz
6C6LcFc2SQLEZKeuTRlhWXS5vjFDMA==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIE0DCCA7igAwIBAgIBBzANBgkqhkiG9w0BAQsFADCBgzELMAkGA1UEBhMCVVMx
EDAOBgNVBAgTB0FyaXpvbmExEzARBgNVBAcTClNjb3R0c2RhbGUxGjAYBgNVBAoT
EUdvRGFkZHkuY29tLCBJbmMuMTEwLwYDVQQDEyhHbyBEYWRkeSBSb290IENlcnRp
ZmljYXRlIEF1dGhvcml0eSAtIEcyMB4XDTExMDUwMzA3MDAwMFoXDTMxMDUwMzA3
MDAwMFowgbQxCzAJBgNVBAYTAlVTMRAwDgYDVQQIEwdBcml6b25hMRMwEQYDVQQH
EwpTY290dHNkYWxlMRowGAYDVQQKExFHb0RhZGR5LmNvbSwgSW5jLjEtMCsGA1UE
CxMkaHR0cDovL2NlcnRzLmdvZGFkZHkuY29tL3JlcG9zaXRvcnkvMTMwMQYDVQQD
EypHbyBEYWRkeSBTZWN1cmUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5IC0gRzIwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC54MsQ1K92vdSTYuswZLiBCGzD
BNliF44v/z5lz4/OYuY8UhzaFkVLVat4a2ODYpDOD2lsmcgaFItMzEUz6ojcnqOv
K/6AYZ15V8TPLvQ/MDxdR/yaFrzDN5ZBUY4RS1T4KL7QjL7wMDge87Am+GZHY23e
cSZHjzhHU9FGHbTj3ADqRay9vHHZqm8A29vNMDp5T19MR/gd71vCxJ1gO7GyQ5HY
pDNO6rPWJ0+tJYqlxvTV0KaudAVkV4i1RFXULSo6Pvi4vekyCgKUZMQWOlDxSq7n
eTOvDCAHf+jfBDnCaQJsY1L6d8EbyHSHyLmTGFBUNUtpTrw700kuH9zB0lL7AgMB
AAGjggEaMIIBFjAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBBjAdBgNV
HQ4EFgQUQMK9J47MNIMwojPX+2yz8LQsgM4wHwYDVR0jBBgwFoAUOpqFBxBnKLbv
9r0FQW4gwZTaD94wNAYIKwYBBQUHAQEEKDAmMCQGCCsGAQUFBzABhhhodHRwOi8v
b2NzcC5nb2RhZGR5LmNvbS8wNQYDVR0fBC4wLDAqoCigJoYkaHR0cDovL2NybC5n
b2RhZGR5LmNvbS9nZHJvb3QtZzIuY3JsMEYGA1UdIAQ/MD0wOwYEVR0gADAzMDEG
CCsGAQUFBwIBFiVodHRwczovL2NlcnRzLmdvZGFkZHkuY29tL3JlcG9zaXRvcnkv
MA0GCSqGSIb3DQEBCwUAA4IBAQAIfmyTEMg4uJapkEv/oV9PBO9sPpyIBslQj6Zz
```


[56] Vide ACP promovida pelo MPDFT contra o Banco Inter (pág.06). Disponível em: < http://www.mpdft.mp.br/portal/pdf/noticias/julho_2018/A%C3%A7%C3%A3o_Danos_Banco_Inter_CS.pdf> e <http://pastebin.xyz/p?q=Vm9iVWw> Acesso em: 22 set. 2018

```
91cxG7685C/b+LrTW+C05+Z5Yg4MotdqY3MxtfWoSKQ7CC2iXZDXtHwlTxFWMMS2
RJ17LJ3lXubvDGGqv+QqG+6EnriDfcFDzkSnE3ANkR/0yBOtg2DZ2HKocyQetawi
DsoXiWJYRBuriSUBAA/NxBti21G00w9RKpv0vHP8ds42pM3Z2Czqrpv1KrKQ0U11
GIo/ikGQI31bS/6kA1ibRrLDYGCD+H1QQc7CoZDDu+8CL9IVVO5EFdkKrqeKM+2x
LXY2JtwE65/3YR8V3Idv7kaWKK2hJn0KCacuBKONvPi8BDAB
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEfTCCA2WgAwIBAgIDG+cVMA0GCSqGSIb3DQEBCwUAMGMxCzAJBgNVBAYTAlVT
MSEwHwYDVQQKExhUaGUgR28gRGFkZHkgR3JvdXAsIEluYy4xMTAvBgNVBAsTKEdv
IERhZGR5IENsYXNzIDIgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwHhcNMTQwMTAx
MDcwMDAwWhcNMzEwNTMwMDcwMDAwWjCBgzELMAkGA1UEBhMCVVMxEDAOBgNVBAgT
B0FyaXpvbmExEzARBgNVBAcTClNjb3R0c2RhbGUxGjAYBgNVBAoTEUdvRGFkZHku
Y29tLCBJbmMuMTEwLwYDVQQDEyhHbyBEYWRkeSBSb290IENlcnRpZmljYXRlIEF1
dGhvcml0eSAtIEcyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAv3Fi
CPH6WTT3G8kYo/eASVjpIoMTpsUgQwE7hPHmhUmfJ+r2hBtOoLTbcJjHMgGxBT4H
Tu70+k8vWTAi56sZVmvigAf88xZ1gDlRe+X5NbZ0TqmNghPktj+pA4P6or6KFWp/
3gvDthkUBcrqw6gElDtGfDIN8wBmIsiNaW02jBEYt9OyHGC0OPoCjM7T3UYH3go+
6118yHz7sCtTpJJiaVElBWEaRIGMLKlDliPfrDqBmg4pxRyp6V0etp6eMAo5zvGI
gPtLXcwy7IViQyU0AlYnAZG0O3AqP26x6JyIAX2f1PnbU21gnb8s51iruF9G/M7E
GwM8CetJMVxpRrPgRwIDAQABo4IBFzCCARMwDwYDVR0TAQH/BAUwAwEB/zAOBgNV
HQ8BAf8EBAMCAQYwHQYDVR0OBBYEFDqahQcQZyi27/a9BUFuIMGU2g/eMB8GA1Ud
IwQYMBaAFNLEsNKR1EwRcbNhyz2h/t2oatTjMDQGCCsGAQUFBwEBBCgwJjAkBggr
BgEFBQcwAYYYaHR0cDovL29jc3AuZ29kYWRkeS5jb20vMDIGA1UdHwQrMCkwJ6Al
oCOGIWh0dHA6Ly9jcmwuZ29kYWRkeS5jb20vZ2Ryb290LmNybDBGBgNVHSAEPzA9
MDsGBFUdIAAwMzAxBggrBgEFBQcCARYlaHR0cHM6Ly9jZXJ0cy5nb2RhZGR5LmNv
bS9yZXBvc2l0b3J5LzANBgkqhkiG9w0BAQsFAAOCAQEAWQtTvZKGEacke+1bMc8d
H2xwxbhuvk679r6XUOEwf7ooXGKUwuN+M/f7QnaF25UcjCJYdQkMiGVnOQoWCcWg
OJekxSOTP7QYpgEGRJHjp2kntFolfzq3Ms3dhP8qOCkzpN1nsoX+oYggHFCJyNwq
9kIDN0zmiN/VryTyscPfzLXs4Jlet0lUIDyUGAzHHFIYSaRt4bNYC8nY7NmuHDKO
KHAN4v6mF56ED71XcLNa6R+ghlO773z/aQvgSMO3kwvIClTErF0UZzdsyqUvMQg3
qm5vjLyb4lddJIGvl5echK1srDdMZvNhkREg5L4wn3qkKQmw4TRfZHcYQFHfjDCm
rw==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEADCCAuigAwIBAgIBADANBgkqhkiG9w0BAQUFADBjMQswCQYDVQQGEwJVUzEh
MB8GA1UEChMYVGhlIEdvIERhZGR5IEdyb3VwLCBJbmMuMTEwLwYDVQQLEyhHbyBE
YWRkeSBDbGFzcyAyIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MB4XDTA0MDYyOTE3
MDYyMFoXDTM0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFRo
ZSBHbyBEYWRkeSBHcm91cCwgSW5jLjExMC8GA1UECxMoR28gRGFkZHkgQ2xhc3Mg
MiBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTCCASAwDQYJKoZIhvcNAQEBBQADggEN
ADCCAQgCggEBAN6d1+pXGEmhW+vXX0iG6r7d/+TvZxz0ZWizV3GgXne77ZtJ6XCA
PVYYYwhv2vLM0D9/AlQiVBDYsoHUwHU9S3/Hd8M+eKsaA7Ugay9qK7HFiH7Eux6w
wdhFJ2+qN1j3hybX2C32qRe3H3I2TqYXP2WYktsqbl2i/ojgC95/5Y0V4evLOtXi
EqITLdiOr18SPaAIBQi2XKVlOARFmR6jYGB0xUGlcmIbYsUfb18aQr4CUWWoriMY
avx4A6lNf4DD+qta/KFApMoZFv6yyO9ecw3ud72a9nmYvLEHZ6IVDd2gWMZEewo+
YihfukEHU1jPEX44dMX4/7VpkI+EdOqXG68CAQOjgcAwgb0wHQYDVR0OBBYEFNLE
sNKR1EwRcbNhyz2h/t2oatTjMIGNBgNVHSMEgYUwgYKAFNLEsNKR1EwRcbNhyz2h
/t2oatTjoWekZTBjMQswCQYDVQQGEwJVUzEhMB8GA1UEChMYVGhlIEdvIERhZGR5
IEdyb3VwLCBJbmMuMTEwLwYDVQQLEyhHbyBEYWRkeSBDbGFzcyAyIENlcnRpZmlj
YXRpb24gQXV0aG9yaXR5ggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQAD
ggEBADJL87LKPpH8EsahB4yOd6AzBhRckB4Y9wimPQoZ+YeAEW5p5JYXMP80kWNy
OO7MHAGjHZQopDH2esRU1/blMVgDoszOYtuURXO1v0XJJLXVggKtI3lpjbi2Tc7P
TMozI+gciKqdi0FuFskg5YmezTvacPd+mSYgFFQlq25zheabIZ0KbIIOqPjCDPoQ
HmyW74cNxA9hi63ugyuV+I6ShHI56yDqg+2DzZduCLzrTia2cyvk0/ZM/iZx4mER
dEr/VxqHD3VILs9RaRegAhJhldXRQLIQTO7ErBBDpqWeCtWVYpoNz4iCxTIM5Cuf
ReYNnyicsbkqWletNw+vHX/bvZ8=
-----END CERTIFICATE-----
Bag Attributes
    friendlyName: star_bancointer_com_br
    localKeyID: 54 69 6D 65 20 31 35 30 33 30 38 35 31 33 31 36 39 36
Key Attributes: <No Attributes>
```

-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQCOrIhVxatF4+tD
Mm2rJXosNYYcV3NHY18Kco0P8Lz2I2V3ULHxcd2AYVk/+LXt0ADBMfs04Ljo7NAT
SGHqxBUOphb0BLPvMSEPoTLxZxd63Z8pvJENLIIrDU9ME1pm4giWxomNhPJYzXfk
17pTylgNbMrxcSOFcXSQvgcHQK3PrABX7aNT6qbqa0EELX36kayGLpxgQ3HBVKWY
QCNztraAmeF9tD+9of2jr0OksibxCJ7n/06n95JefoTd0SaZK7DfzhpvGbHiXRgR
VMKznrmTIV7S4Sju2kemTDuAOOc453rNX1xQJHKeBudO3x36sPDTGj6xvs9ZFkq6
v2Kv/SEvAgMBAAECggEAdMqnkA8P9VZt78QIImG7cRUfg3PS2k1uL482CiZ3iMXQ
+asE/zDGsaD+/m8J/nKXK49OpCqRM5sneaF3BkcdNbCgeYCgCt2cwr6ihRpvDhT9
hZzm4HHe3H84un3dMvs1LLe5Qi/icu8/hgVSceThz5uPRbXn7gTB9vqXpkg8ABL5
hl7hEBYCwrplet6mZ2Zkp+oYQSMB4kZoDUyxkvfs7I36DtIne884O0g1KVPH4Q4R
Y/9ny6LUicNG7lPwnm41hhBXWW1/2SkWC1BB66AyAlCW7l5WZ3XU8EdqahYQmiXq
Wqa0ICeqhi56XxlJe97o7pULVZvUNa1zGPu48o0IgQKBgQD3kgq0WAzVn0aFKlp9
Ar7ClpWCfzyboJ3ENB49spTrcZlffGQF0j9gqE4Eu0h/CxW9bX3bky5F/HmBhCuo
/oUkiH6d300kOp4RTQk6EdKjsqMLfOrQzI9zBIyqRJkBU79rLrotenGd4v393uGb
fvymDiWvR469OIH3NvOTSN27gwKBgQCTiCfrBMP/cXwJ2t+Yaqs7GoMwHpZIZdj1
myhkfwtY0X0UJ0b1NvBzjOZlsKRwcgWTIlFyHMCX/DVWyuW0pAwTAFIEuQEwtMJj
vVEyYG6RjRt8MBFZZ3uil/4zAqpiHWUegVJtBuNDEOKU7hotGY4YKV1XPz7CaUGZ
Cd8eDRP35QKBgFyjJiRDilHpLo8nwQJkI5NWm41gJQKrAD3prqMxjq3nLRfgyOCw
woxdjgwRNFhtgm4GaYDfOwJvLdw748Zxrspz1MUoSIpU8M7Sf7Bd+O7OKlpjHM6S
rN7CBgy0bHhlqQvnST05QwhsZtQ3MT5pLwrH4mwLH6tIWMFzq4MiUe4XAoGADlr8
T2EKVUvMnwTeJu2SNdERnNgNFYRbhSKQ3p6CEyVnP1PHEstCwGuga5qxlYNyyWtY
c3savm87HXPmwBoKVrr8QBtkY0HjfGMKiJVbjOwnFYFz3rg0DpEtmfcTbzKfCUXa
KGO4L2lwMr+samEHM5Cq1XeA+tfVGzgbrsfk/oUCgYAQbxBJww4g0SN8pkUi6giR
5REMyg3kw/IjynPV3gxv/NLlZo0YM2CDllk3GX3gmd8LdamTWtmGRVIQPUWogb1U
Lfy6UOB9ntqqsXZRdAn/yx3VHIoyrHleqVXA4kFN1SpMzWMqSmUQ2rJr2ycpynDV
tirBsPFj9rQQypRC924rXw==
-----END PRIVATE KEY-----