III ENCONTRO VIRTUAL DO CONPEDI

DIREITO INTERNACIONAL II

FLORISBAL DE SOUZA DEL OLMO

VALTER MOURA DO CARMO

CARLA NOURA TEIXEIRA

D597

Direito internacional II [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Carla Noura Teixeira; Florisbal de Souza Del Olmo; Valter Moura do Carmo – Florianópolis: CONPEDI, 2021.

Inclui bibliografia
ISBN: 978-65-5648-330-6
Modo de acesso: www.conpedi.org.br em publicações
Tema: Saúde: segurança humana para a democracia

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Internacional. III Encontro Virtual do CONPEDI (1: 2021 : Florianópolis, Brasil).

CDU: 34

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

III ENCONTRO VIRTUAL DO CONPEDI

DIREITO INTERNACIONAL II

Apresentação

Texto de Apresentação – GT Direito Internacional II

O Direito Internacional na contemporaneidade tem oferecido reflexões para além da arena tradicional das relações interestatais, apresentando relações jurídicas, por vezes privadas com interesse público ou públicas com a presença de novos sujeitos internacionais como as organizações não governamentais e o indivíduo. A observância de tal cenário rompe qualquer alocação primeira nas áreas de Direito Internacional Público, Direito Internacional Privado ou Direito Internacional do Comércio, e exsurge em temas voltados a Teoria do Direito Internacional, as fontes jurídicas, aos princípios regentes, bem como a ética aplicada as relações internacionais, bem como o papel das Organizações Internacionais no século XXI e a sistemática de funcionamento e enfrentamento em face os desafios globais permeados pela Tecnologia, a mudança das relações de trabalho e a globalização, sem olvidar a situação da pandemia pelo coronavírus COVID-19.

Durante o III Encontro Virtual do Conselho Nacional de Pesquisa e Pós-Graduação em Direito (CONPEDI), realizado virtualmente em junho de 2021, foi realizado o Grupo de Trabalho (GT) Direito Internacional II. A presente publicação é fruto de parte dos artigos apresentados, já que alguns foram encaminhados aos periódicos do Index Law Journals. Eis o trabalhos apresentados:

Lucas David Campos De Siqueira Camargo, Miguel Mendes Filho e Paulo Marcio Reis Santos apresentam o artigo intitulado “O PADRÃO ÉTICO COMO REQUISITO DE CONFORMIDADE NOS CONTRATOS DE NA COMPRA E VENDA INTERNACIONAL”, versando sobre a Convenção das Nações Unidas sobre Contratos de Compra e Venda Internacional de Mercadorias, questionando se configuram um rol exemplificativo ou taxativo, indicando a observância de padrões éticos para se aferir a conformidade.

Na sequência tem-se o artigo “VAZAMENTO DE DADOS PESSOAIS ATRAVÉS DE EMPRESAS DE TELEFONIA E A LGPD: ANÁLISE COMPARADA ENTRE AS INICIATIVAS DAS AGÊNCIAS REGULADORAS BRASILEIRA, EUROPEIA E NORTE-AMERICANA”, de autoria de Mariana Weba Lobato Vaz, Kelton Felipe Carvalho de Santana e Florisbal de Souza Del Olmo que aborda uma comparação entre as agências

reguladoras de proteção de dados pessoais do Brasil, União Europeia e Estados Unidos da América. Busca-se evidenciar através das legislações de cada um desses entes governamentais o tratamento que seria realizado com as empresas de telefonia caso ocorresse um incidente de segurança. O artigo "WIKILEAKS: A AUSÊNCIA DE REGULAMENTAÇÃO DOS CONTEÚDOS PUBLICADOS NA INTERNET" de autoria de João Pedro Carvalho de Barros apresenta a discussão sobre a responsabilidade por publicações on-line, mais precisamente com relação ao Wikileaks e a falta de regulamentação Internacional a respeito da divulgação dessas informações, para ao final propor a necessidade de regulamentação Internacional, pela alternativa de um Tratado.

O artigo "LIMITES PARA A LIBERDADE DE REUNIÃO E A AUTONOMIA PRIVADA: FUNDAMENTOS EM CONVENÇÕES INTERNACIONAIS DE DIREITOS HUMANOS" de Mario Jorge Philocreon De Castro Lima e Keyla Cristina Farias Dos Santos traz o contexto da pandemia pelo COVID-19 para observar a aplicação de medidas restritivas que afetam liberdades individuais, oferecendo soluções compatíveis encontradas nas convenções internacionais de direitos humanos, pela utilização de cláusulas de exceção, pela demanda de deveres fundamentais, ou pela promoção de soluções jurídicas de proporcionalidade entre normas internacionais de mesmo valor. No âmbito de cooperação internacional tem-se o artigo "O APOSTILAMENTO DE HAIA COMO FONTE DE COOPERAÇÃO JURÍDICA INTERNACIONAL" de Beatriz Peixoto Nóbrega e Ivanka Franci Delgado Nobre em que buscam demonstrar como os atos e informações expedidos pelos notários brasileiros podem ser utilizados como mecanismos de cooperação jurídica internacional.

Na linha de artigos acerca da homologação de sentença estrangeira o artigo "EM MATÉRIA TRABALHISTA, A COMPETÊNCIA PARA HOMOLOGAÇÃO DE SENTENÇA ESTRANGEIRA DEVERIA SER DO TRIBUNAL SUPERIOR DO TRABALHO?" de autoria de Tiago Batista dos Santos, Ricardo Galvão de Sousa Lins e Yara Maria Pereira Gurgel busca investigar se a competência para homologação de sentença estrangeira em matéria trabalhista deveria ser do TST. E o "(IR)RESPONSABILIDADE CORPORATIVA E A COGNIÇÃO (I)LIMITADA NA HOMOLOGAÇÃO DE SENTENÇAS ESTRANGEIRAS: UM ESTUDO DA SEC Nº 8.542 (CASO CHEVRON-TEXACO – AMAZON CHERNOBYL) de Renan de Marco D'Andréa Maia e Cynthia Soares Carneiro verifica, a partir da análise da SEC nº 8.542 (Caso Chevron-Texaco), o entendimento do Superior Tribunal de Justiça sobre a extensão do juízo de delibação na homologação de sentenças estrangeiras.

Apresentando as Organizações Internacionais o artigo "MODERNIZAÇÃO DA ORGANIZAÇÃO MUNDIAL DO COMÉRCIO (OMC): PROPOSTAS DE ALTERAÇÕES

NO FUNCIONAMENTO DO “DISPUTE SETTLEMENT BODY – DSB”” de autoria de Matheus Fernandino Bonaccorsi descreve a necessidade de modernização do Dispute Settlement Body no âmbito da Organização Mundial do Comércio a partir das propostas da União Européia. Por seu turno, o artigo “OPINIÃO CONSULTIVA 26/2020 DA CORTE INTERAMERICANA DE DIREITOS HUMANOS: SUBSISTEM OBRIGAÇÕES INTERNACIONAIS DE DIREITOS HUMANOS AO ESTADO-MEMBRO DA OEA QUE DENUNCIA A CONVENÇÃO AMERICANA DE DIREITOS HUMANOS?” de Eneida Orbage De Britto Taquary e Catharina Orbage De Britto Taquary Berino refere-se as obrigações que subsistem ao Estado-membro da Organização dos Estados Americanos que denuncia a Convenção Americana de Direitos Humanos.

A autora Mariangela Ariosi apresenta o artigo intitulado “A TEORIA CLÁSSICA DA SOBERANIA NAS RELAÇÕES ENTRE O DIREITO INTERNACIONAL E O DIREITO INTERNO: UMA ANÁLISE DAS REGRAS DESSA RELAÇÃO NA CONSTITUIÇÃO FEDERAL” apresenta panorama dos estudos das relações entre o Direito Internacional – DI e o Direito Interno representando a soberania um papel de interface dessa relação; ademais, uma breve transcrição das duas principais teorias clássicas que se dedicam a explicar essa relação: monista e dualista.

Na sequência, o artigo “COSMOPOLITISMO JURÍDICO: DIRETRIZES GERAIS PARA A PROPOSITURA DE UM DIREITO DO TRABALHO GLOBAL” de Stéfani Clara da Silva Bezerra, Alexandre Antonio Bruno da Silva e Amanda Ingrid Cavalcante de Morais apresenta a possibilidade de um compartilhamento de valores a nível mundial no âmbito do trabalho, sob a égide da teoria do Cosmopolitismo Jurídico, na construção de um Direito do Trabalho Global.

O artigo “TESOUROS DE ÁFRICA PELO MUNDO: A RESTITUIÇÃO DE PATRIMÔNIO CULTURAL FRENTE AO DIREITO INTERNACIONAL” de Juliana Muller e Carolina Nunes Miranda Carasek da Rocha analisa as restituições de bens culturais originários do continente africano frente ao Direito Internacional, no texto é explorada a alienação do patrimônio originário dos povos da África e é demonstrada a legislação internacional aplicável a estes objetos de valor.

Augusto Guimarães Carrijo e Tatiana de Almeida Freitas Rodrigues Cardoso Squeff, autores do artigo “ATAQUES DIRECIONADOS ÀS FONTES DE MÍDIA DURANTE CONFLITOS ARMADOS: UMA ANÁLISE DO BOMBARDEAMENTO DA ESTAÇÃO RTS NA EX-IUGOSLÁVIA CONSOANTE O DIREITO INTERNACIONAL HUMANITÁRIO” debatem a possibilidade de estações midiáticas serem considerados alvos

legítimos, passíveis de sofrerem ataques em meio a hostilidades, observando o caso do bombardeio realizado pelas tropas da Organização do Tratado do Atlântico Norte à Estação de Rádio e Televisão da Sérvia durante a guerra do Kosovo em 1999, utilizando-se como base analítica as regras do I Protocolo Adicional e as interpretações de tribunais internacionais.

O artigo “AS CONTRIBUIÇÕES DO COSMOPOLITISMO SUBALTERNO AO DIREITO INTERNACIONAL” de Gabriel Pedro Moreira Damasceno traz a análise das contribuições do Cosmopolitismo Subalterno ao Direito Internacional, buscando-se uma conceptualização cosmopolita descolonial alternativa do sistema-mundo. Por derradeiro, o artigo “A ORDEM MUNDIAL ESTÁ CONTAMINADA - A GLOBALIZAÇÃO SOBREVIVERÁ À ATUAL PANDEMIA?” de Chantal Correia de Castro compartilha um questionamento: o mundo polarizado, cuja antiga ordem já se encontrava ameaçada, foi atingido pelo vírus mais globalizado da história. Os sintomas como populismo e protecionismo que já se manifestavam foram agravados e o Covid-19 pode representar o golpe fatal para a globalização e a ordem multilateral. Que tipo de ordem internacional emergirá em um mundo pós-pandemia?.

Por todos os temas aqui reunidos, demonstra-se que as questões que antes eram locais estão cada vez mais globais e instam os pesquisadores internacionalistas - cientistas do Direito - à investigação, a reflexão e ao enfrentamento propositivo de soluções para o bem-viver coletivo.

O desafio está posto!

Em tudo, indica-se como bom começo a leitura dos artigos aqui reunidos.

Profa Dra Carla Noura Teixeira – UNAMA – carlanoura@gmail.com

Prof. Dr. Florisbal de Souza Del Olmo – UNICURITIBA – florisbaldelolmo@gmail.com

Prof. Dr. Valter Moura do Carmo – Universidade de Marília – vmcarmo86@gmail.com

VAZAMENTO DE DADOS PESSOAIS ATRAVÉS DE EMPRESAS DE TELEFONIA E A LGPD: ANÁLISE COMPARADA ENTRE AS INCIATIVAS DAS AGÊNCIAS REGULADORAS BRASILEIRA, EUROPEIA E NORTE-AMERICANA

LEAKAGE OF PERSONAL DATA THROUGH TELEPHONE COMPANIES AND THE LGPD: COMPARATIVE ANALYSIS BETWEEN THE ACTIVITIES OF THE BRAZILIAN, EUROPEAN AND NORTH AMERICAN REGULATORY AGENCIES

Mariana Weba Lobato Vaz [1]
Kelton Felipe Carvalho de Santana [2]
Florisbal de Souza Del Olmo [3]

Resumo

O artigo trata de uma comparação entre as agências reguladoras de proteção de dados pessoais do Brasil, União Europeia e Estados Unidos da América. Busca-se evidenciar através das legislações de cada um desses entes governamentais o tratamento que seria realizado com as empresas de telefonia caso ocorresse um incidente de segurança. A caso adotado para comparação ocorreu no Brasil no dia 10 de fevereiro de 2021 pelo vazamento de dados pessoais e telefônicos de milhões de brasileiros pelas empresas telefônicas Claro, Oi, Vivo e Tim. O método de pesquisa é dedutivo, com análise de caso, sendo uma pesquisa exploratória.

Palavras-chave: Proteção de dados, Agências reguladoras, Anpd, Consumidor, Incidentes de segurança

Abstract/Resumen/Résumé

The article deals with a comparison between the regulatory agencies for the protection of personal data in Brazil, the European Union and the United States of America. It seeks to highlight through the laws of each of these governmental entities the treatment that would be carried out with telephone companies if a security incident occurred. The case adopted for comparison occurred in Brazil on February 10, 2021 by the leakage of personal and telephone data of millions of Brazilians by the telephone companies Claro, Oi, Vivo and Tim. The research method is deductive, with case analysis, being an exploratory research.

[1] Mestranda em Direito, Compliance, Mercado e Segurança Humana, pela Faculdade CERS. Especialista em Direito de Família, da Infância e Juventude pela UNDB. Mediadora e Conciliadora Judicial. Residente Jurídica do TJ/MA.

[2] Mestrando em Direito, Compliance, Mercado e Segurança Humana, pela Faculdade CERS. Especialista em Direito e Processo do Trabalho e Direito Previdenciário. Advogado.

[3] Pós-doutor em Direito pela UFSC. Doutor em Direito pela UFRGS. Mestre em Direito pela UFSC. Professor convidado da UFRGS. Associado honorário do CONPEDI.

Keywords/Palabras-claves/Mots-clés: Data protection, Regulatory agencies, Anpd, Consumer, Security incidents

1. Introdução

O tratamento de dados pessoais no Brasil tem sido um ponto extremamente discutido devido aos diversos ataques de hackers sofridos pelas empresas brasileiras e órgãos públicos nos últimos meses. Inicialmente um ataque hacker que apagou todas as informações processuais do sistema do Superior Tribunal de Justiça (STJ), posteriormente o vazamento de uma lista de dados contendo dados sensíveis em massa de brasileiros, a qual ainda não se sabe a proveniência. E posteriormente e foco deste artigo o vazamento de dados sensíveis de quatro grandes empresas de telefonia brasileiras: a Claro, Oi, Vivo e Tim, no dia 10 de fevereiro de 2020.

O Procon/SP no dia 17 de fevereiro de 2021 notificou as empresas para que as mesmas justificassem o vazamento de dados dos clientes. Diante disto, alguns esclarecimentos necessitam ser feitos acerca de como seria o tratamento da autoridade reguladora brasileira diante desta situação com as empresas de telefonia. Para isto, diante das influências que o Direito Brasileiro segue a partir do Direito europeu, e também do avanço significativo da legislação europeia sobre este assunto, far-se-á um comparativo de como as autoridades nacionais de cada um desses países se comportaria diante de tal situação, esclarecendo assim um pouco do vácuo existente quanto a ação da Autoridade Nacional de Proteção de Dados (ANDPD) no Brasil.

Posto isso, diante do numero crescente de casos que relatam incidentes de segurança, é necessária uma pesquisa que traga parâmetros jurídicos que protejam os consumidores destes incidentes. De tal modo, o tema que trata incidentes de segurança ainda é raso e pouco discutido no Brasil, necessitando de um maior desenvolvimento que auxilie na tomada de decisões tanto da Agencia Nacional de Proteção de Dados do Brasil, quanto de órgãos do executivo e até mesmo judiciário ao se verem impactados por tais incidentes.

O método utilizado para elaboração do artigo foi o dedutivo, através de uma análise do caso concreto escolhido de forma aleatória e de uma pesquisa exploratória, com busca de bibliografias que pudessem substanciar a pesquisa.

2. Vazamento de dados pessoais de clientes de empresas de telefonia brasileiras e a LGPD

No dia 10 de fevereiro de 2021 o Brasil sofreu um grande ataque cibernético quando ao vazamento de dados pessoais de clientes das empresas de telefonia CLARO, OI, VIVO e TIM. Um grupo hacker ao conseguir um acesso identificou e listou todos os dados de clientes

dessas empresas telefônicas e disponibilizou abertamente na *dark web*[1]. Tal ataque não tem uma motivação exposta, mas o fato é que as empresas de telefonia devem ser responsáveis por este vazamento, pois tem a obrigação de manter tais dados em sigilo e protegidos. Por isso, o PROCON/SP, ao notificar as empresas requereu a confirmação acerca do vazamento de dados pessoais de suas bases, os motivos do incidente, e em detalhes as medidas cabíveis para conter o vazamento e quais as medidas de reparação dos danos causados pelo incidente. O Procon/SP, também notificou a empresa de segurança digital Psafe, que confirmou o vazamento de mais de 103 milhões de contas telefônicas disponibilizadas na *dark web* requerendo que a empresa explique como se deu o contato com hacker que noticiou o vazamento, quais informações foram vazadas e se o vazamento se deu apenas na *dark web*.

No vazamento os clientes das empresas telefônicas tiveram seus dados de RG, CPF, data de nascimento, e-mail, endereço, número de celular, de detalhes de suas faturas disponibilizados. Na notificação do Procon/SP para as empresas foi indagada a base de dados pessoais para tratamento de dados, política de descarte e armazenamento de dados, além de medidas técnicas organizacionais que são tomadas para cumprimento das diretrizes da LGPD.

Diante desta situação alguns pontos precisam ser esclarecidos para que se entenda a atitude do Procon/SP. Tais dados vazados, sendo eles: RG, CPF, data de nascimento, e-mail, endereço, número de celular, de detalhes de suas faturas, são considerados dados pessoais segundo o art. 5º, I, da Lei 13.709/2018 (Lei Geral de Proteção de Dados).

Segundo esta lei em seu art. 6º, VII, ao tratamento de dados pessoais deve ser garantido, além da boa-fé e demais princípios a segurança, que seria a "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão".

As empresas de telefonia entram como as operadoras e controladoras do tratamento de dados pessoais, sendo elas um dos agentes de tratamento segundo o art. 5º, VI, VII, IX, X, da LGPD, cabendo a elas manter a segurança do banco de dados do titular, ou seja, da "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento"(BRASIL, 2018).

É importante salientar, que os clientes ao realizarem o contrato com as empresas de telefonia, fornecem a eles o seu consentimento, que é definido pelo art. 5º, XII da LGPD como: "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".

[1] A Dark é o nome dado para a parte obscura da Deep Web. Por não ser um lugar controlado, é onde normalmente são encontrados conteúdos ilícitos, como bens roubados, armas, drogas, etc.

Esse tratamento de dados pelas empresas de telefonia, se torna legitimo por força do art. 7º, I e V, da LGPD, que além do consentimento garante a possibilidade de tratamento "quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados".

O Procon/SP por força do art. 22, da LGPD, possui competência para deliberar processos judiciais cabíveis, garantindo a defesa dos interesses e dos direitos dos titulares de dados.

Além disto, no art. 38, fica claro que:

> A autoridade nacional poderá determinar ao controlador que elabore **relatório de impacto à proteção de dados pessoais**, inclusive de dados sensíveis**, referente a suas operações de tratamento de dados**, nos termos de regulamento, observados os segredos comercial e industrial.
>
> Parágrafo único. Observado o disposto no caput deste artigo, **o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados** (BRASIL, 2018).

Observa-se que o artigo trata da Autoridade Nacional de Proteção de Dados, autoridade está um pouco omissa no Brasil e em sua ausência o Procon/SP, tem agido requerendo tais informações das empresas telefônicas, para garantir que a responsabilidade exposta no art. 42, da LGPD, seja garantida, já que "o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo." Ainda há de se falar ainda na possibilidade de responsabilização através do uso do CDC/1990, pois o artigo 45 da LGPD mantém a possibilidade do uso da legislação pertinente nos casos de violação nas relações de consumo.

Para garantia sobre segurança e sigilo de dados a LGPD traz em seu bojo como os agentes de tratamento devem agir, onde dispõe nos artigos abaixo:

> **Art. 46.** Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
>
> § 1º **A autoridade nacional** poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

> § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.
>
> **Art. 47.** Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.
>
> **Art. 48.** O controlador deverá comunicar à **autoridade nacional** e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
>
> § 1º A comunicação será feita em prazo razoável, conforme definido pela **autoridade nacional**, e deverá mencionar, no mínimo:
>
> I - a descrição da natureza dos dados pessoais afetados;
>
> II - as informações sobre os titulares envolvidos;
>
> III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
>
> IV - os riscos relacionados ao incidente;
>
> V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
>
> VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.
>
> § 2º **A autoridade nacional** verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:
>
> I - ampla divulgação do fato em meios de comunicação; e
>
> II - medidas para reverter ou mitigar os efeitos do incidente.
>
> § 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.
>
> **Art. 49.** Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares (BRASIL, 2018)

O que se observa é uma série de diretrizes de segurança que devem ser estabelecidas, neste caso, pelas empresas de telefonia, as quais o Procon/SP em sua notificação fez questão de agir de forma a questionar a segurança destas empresas.

Diante de toda essa explanação, o ponto a ser tocado é que em nenhum momento houve uma atitude a partir de uma Autoridade Nacional de Proteção de Dados, mas sim uma atuação do Procon/SP. É importante destacar que no bojo da LGPD não se fala da atuação do Procon, mas sim da ANPD, instituição essa criada por forma da LGPD, mas que não tem atuado

no Brasil, a qual o Procon tem substituído para fazer as devidas correções, garantindo a proteção dos consumidores.

Ocorre que, recentemente a ANPD aprovou a Portaria nº 21 de 27 de janeiro de 2021 (BRASIL, 2021b), que prevê como meta em seu item nº 06 um início de processo de regulamentação sobre incidentes de segurança. Essa iniciativa se dá pela Tomada de Subsídios (BRASIL, 2021a), onde possibilita a participação da sociedade durante as frases preliminares de um processo regulatório dessa Autoridade.

Juntamente a esta portaria, a ANPD disponibilizou um formulário[2] para comunicação de incidentes de segurança de dados pessoais, e também um documento com orientações sobre o que fazer em caso de um incidente de segurança. Esses documentos servem como um guia, enquanto a regulamentação está sendo elaborada conjuntamente com a tomada de subsídios.

Essa movimentação da ANPD, demonstra na verdade o início do processo de regulamentação e da tomada de atitudes acerca dos incidentes de segurança, como este de vazamento de dados telefônicos. Até o presente momento devem ser notificados a ANPD os incidentes, contendo todas as informações requisitadas no art.48, §1º, da LGPD, mediante o formulário disponível no site através do link: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca.

Porém, apesar de todas essas novidades acerca do papel e das atitudes da ANPD, o ponto sensível quanto a isto é a legitimidade do Procon/SP para garantir as sanções administrativas previstas na LGPD, pois não cabe a ele estas sanções. Um ponto crucial, pois a eficácia da garantia de segurança de dados pessoais dos consumidores fica limitada a atuação legitima do Procon, não possuindo sequer uma atitude da autoridade nacional eficaz para a regulamentação das atividades dessas empresas, seja para autorizar, seja para garantir, ou para fiscalizar a atuação destas empresas.

Para uma análise crítica, nos próximos tópicos será abordado a atuação da Autoridade Europeia de Proteção de Dados e das agências norte-americanas que atuam na proteção de dados, a FTC e na proteção de comunicações telefônicas a FCC.

3. Supervisor Europeu de Proteção de Dados (EDPS)

Na União Europeia, entrou em vigor o Regulamento Geral de Proteção de Dados (GDPR) em 05 de maio de 2016, uma das maiores conquistas nos últimos anos, substituindo

[2] Comunicação de incidentes de segurança. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca.

então a Diretiva de Proteção de Dados de 1995. O GDPR é reconhecido hoje como legislação em toda a União Europeia e foi instituído para que em até 06 de maio de 2018 todos os países o implementassem.

Em consonância a toda a política de proteção de dados foi criada em 2004 o Supervisor Europeu de Proteção de Dados ou European Data Protection Supervisor (EDPS) e cada país criou órgãos nacionais responsáveis pela proteção de dados pessoais de acordo com o art. 8º da Carta de Direitos Fundamentais da União Europeia, sendo eles as Autoridades de Proteção de Dados (DPA's).

Além disto, foi criado o Conselho Europeu de Proteção de Dados (EDPB), organismo esse independente que garante a aplicação eficaz das regras de proteção de dados em toda a união europeia. Conselho este criado pelo GDPR, sendo ele constituído pelos representantes das autoridades nacionais de proteção de dados de cada um dos países da UE e do Supervisor Europeu de Proteção de Dados.

Na Europa existe o Oficial de Proteção de Dados encarregado de monitorar e aplicar as regras de proteção de dados na Comissão Europeia. Ele garante a aplicação interna das regras de proteção de dados em cooperação com o EDPS de forma independente.

O papel do EDPS é garantir que as instituições e organismos de UE respeitem o direito à privacidade das pessoas ao processar seus dados pessoais. Esse processamento inclui coletar, gravar, armazenar, recuperar, enviar, bloquear ou apagar dados, ficando como competência do Supervisor Europeu de Proteção de Dados a garantia as regras de privacidade.

Sendo assim, o EDPS tem 04 funções, sendo elas:

> Supervisionar o processamento de dados pessoais pela administração da UE para garantir o cumprimento das regras de privacidade; aconselhar Instituições e organismos da UE sobre todos os aspectos do processamento de dados pessoais e políticas e legislações relacionadas; lidar com reclamações e realiza inquéritos; trabalhar com as autoridades nacionais dos países da UE para garantir a consistência na proteção de dados; monitorar novas tecnologias que podem ter impacto na proteção de dados.[3]

O EDPS também funciona em duas frentes: supervisão e fiscalização e política e consulta. A supervisão e fiscalização "avalia a conformidade com a proteção de dados por

[3] Supervises the EU administration's processing of personal data to ensure compliance with privacy rules; advises EU institutions and bodies on all aspects of personal data processing and related policies and legislation; handles complaints and conducts inquiries; works with the national authorities of EU countries to ensure consistency in data protection; monitors new technologies that might have an impact on data protection. Tradução nossa.

instituições e órgãos da UE"[4] e a política e consulta "aconselha os legisladores da UE sobre questões de proteção de dados em várias áreas políticas e novas propostas legislativas"[5].

Assim, se você tiver um direito à privacidade violado por instituição ou órgão da UE, você deve buscar um funcionário da UE responsável pelo processamento de seus dados onde você acredite que o incidente foi cometido, e se não estiver satisfeito você pode buscar o Oficia de Proteção de Dados da instituição ou órgão da UE que cometeu o incidente. Se todas essas possibilidades falharem é possível se fazer uma reclamação formal ao EDPS, através do formulário de submissão de reclamações, onde o Supervisor Europeu realizará uma investigação e informará sobre a concordância com a reclamação e como ela poderá ser corrigida caso seja confirmada. Caso se discorde da decisão do EDPS, o assunto poderá ser levado até o Tribunal de Justiça da União Europeia (UNIÃO EUROPEIA, 2021).

Diante dessas informações então: como seria tratado o problema do vazamento de dados de empresas de telefonia na União Europeia?

Segundo o regulamento 2016/679 da UE, no art. 51 cada Estado – Membro da UE, irá criar sua autoridade de controle responsável por representar sua autoridade no comitê e assegurar as regras relativas a este regulamento em seu respectivo estado. suas atribuições previstas no art. 57 deste regulamento, incluem todas as listadas e mais quaisquer outras tarefas que se relacionem a proteção de dados pessoais.

É importante esclarecer que essas autoridades de controle que garantem o recebimento das reclamações quanto a violação de dados e possui poderes, estes descritos no art. 58 deste regulamento que garantem a investigação, correção, consulta e autorização acerca do tratamento de dados pelos órgãos, ou empresas. Sendo assim no mesmo artigo ainda se prevê:

> 4. O exercício dos poderes conferidos à autoridade de controlo nos termos do presente artigo está sujeito a garantias adequadas, que incluem o direito à ação judicial efetiva e a um processo equitativo, previstas no direito da União e dos Estados-Membros, em conformidade com a Carta.
>
> 5. Os Estados-Membros estabelecem por lei que as suas autoridades de controlo estão habilitadas a levar as violações do presente regulamento ao conhecimento das autoridades judiciais e, se necessário, a intentar ou de outro modo intervir em processos judiciais, a fim de fazer aplicar as disposições do presente regulamento.

[4] Supervision and Enforcement - evaluates data protection compliance by EU institutions and bodies. Tradução nossa.

[5] Policy and Consultation - advises EU legislators on data protection issues in various policy areas and new legislative proposals. Tradução nossa.

> 6. Os Estados-Membros podem estabelecer por lei que as suas autoridades de controlo terão outros poderes para além dos previstos nos n.os 1, 2 e 3. O exercício desses poderes não deve prejudicar o efetivo funcionamento do capítulo VII (UNIÃO EUROPEIA, 2016)

Ademais, as autoridades de controle podem ser mais de 01 a depender de cada Estado – Membro, o que não impede a atuação de uma ou outro, mas garante a assistência mútua entre elas, nos arts. 60 e 61 da diretiva supracitada, garantindo que a autoridade de controle principal possa trabalhar conjuntamente as autoridades de controle interessadas.

O ponto crucial a ser tratado aqui é trazido pelos arts. 82, 83 e 84, do regulamento 2016/679 da UE. São os artigos que tratam do direito da indenização e responsabilidade, das condições gerais para aplicação de Coimas e das sanções, respectivamente pela violação de dados pessoais.

O art. 82, n.01 prevê que "qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do presente regulamento tem direito a receber uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos." Os pontos seguintes preveem em complementação que:

> 2. Qualquer responsável pelo tratamento que esteja envolvido no tratamento é responsável pelos danos causados por um tratamento que viole o presente regulamento. O subcontratante é responsável pelos danos causados pelo tratamento apenas se não tiver cumprido as obrigações decorrentes do presente regulamento dirigidas especificamente aos subcontratantes ou se não tiver seguido as instruções lícitas do responsável pelo tratamento.
>
> 3. O responsável pelo tratamento ou o subcontratante fica isento de responsabilidade nos termos do n.º 2, se provar que não é de modo algum responsável pelo evento que deu origem aos danos.
>
> 4. Quando mais do que um responsável pelo tratamento ou subcontratante, ou um responsável pelo tratamento e um subcontratante, estejam envolvidos no mesmo tratamento e sejam, nos termos dos n.ºs 2 e 3, responsáveis por eventuais danos causados pelo tratamento, cada responsável pelo tratamento ou subcontratante é responsável pela totalidade dos danos, a fim de assegurar a efetiva indemnização do titular dos dados.
>
> 5. Quando tenha pago, em conformidade com o n.º 4, uma indemnização integral pelos danos sofridos, um responsável pelo tratamento ou um subcontratante tem o direito de reclamar a outros responsáveis pelo tratamento ou subcontratantes envolvidos no mesmo tratamento a parte da indemnização correspondente à respetiva parte de responsabilidade pelo dano em conformidade com as condições previstas no n.º 2.

> 6. Os processos judiciais para exercer o direito de receber uma indemnização são apresentados perante os tribunais competentes nos termos do direito do Estado-Membro a que se refere o artigo 79º, n.º 2 (UNIÃO EUROPEIA, 2016).

Regulamentação esta que se equipara a estabelecida pela LGPD, pois responsabiliza os envolvidos no tratamento de dados por qualquer violação de dados previstas no regulamento, ou no caso da LGPD, prevista na LGPD. O subcontratante tratado do regulamento seria o responsável por garantir a segurança do tratamento de dados pessoais, figura esta que não existe na LGPD, mas entra como princípio do agente de tratamento de dados pessoais, quais sejam o controlador e o operador, no Brasil.

Seguindo ainda a aplicação das Coimas, ou seja, multas, cada autoridade de controle assegura a aplicação das coimas diante de uma violação na segurança do tratamento de dados. As coimas variam entre 10.000.000 EUR até 20.00.000 EUR ou de 2% (dois porcento) a 4% (quatro porcento) do volume de negócios anual a nível mundial das empresas, correspondente ao exercício financeiro anterior, de acordo com o montante mais elevado, tendo estas variações situações específicas para cada valor. No Brasil, a LGPD determina valores a partir de 2% (dois porcento) do faturamento da pessoa jurídica de direito público ou privado, grupo ou conglomerado no Brasil, limitando ao limite de R$50.000.000,00 (cinquenta milhões de reais) e alguns critérios de estabelecimento dos valores indenizatórios, de acordo com os art. 52 da LGPD.

Em consonância a isto, na UE, cada Estado -membro a depender do seu sistema-jurídico pode prever coimas de valores diferenciados, mas caso não tenha previsão, observa-se este regulamento.

Quanto as sanções os Estados-Membros estabelecem regras relativas a outras sanções em caso de violação do regulamento 2016/169, desde que não sujeitas as coimas previstas nos termos dos artigos 79 à 83 e eles mesmos tomam as medidas para aplicação das sanções, devendo elas serem efetivas, proporcionais e dissuasivas (DOHMANN, 2021).

Sendo assim, diante de um possível vazamento de dados pelas empresas telefônicas como aconteceu no Brasil, o primeiro ponto a se analisar seria a amplitude do vazamento, se este se deu somente em determinado Estado-membro da UE, o que ficaria sobre competência da autoridade de controle deste Estado, e esta definiria a indenização válida, diante dos critérios estabelecidos no art. 83, nº 2, do regulamento 2016/169.

Porém, se a situação se esvaiu atingindo todos os Estados -Membros da UE, o que passar-se-ia então a ficar a cargo da UEPD em sessão conjunta com o EDPB que então iriam definir como seria viabilizada a investigação e supervisão das empresas, através de inquérito

que se avalia a reclamação e a partir disso iriam definir uma indenização de maneira mais adequada.

Além disto, a imposição de multas pelos órgãos reguladores, ou seja, agentes controladores, não é impeditivo, onde observado o descumprimento dos regulamentos quanto a proteção de dados, as empresas podem ser condenadas a multas que ultrapassam os 500.000.000 EUR (quinhentos milhões de euros), como no caso do Twitter, em 2019, onde a Comissão de Proteção de Dados da Irlanda é o principal órgão regulador das empresas Twitter, Facebook, Apple e Google pela localização de suas sedes.

Além desta diretiva, a UE estabeleceu o regulamento 2008/52, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações electrónicas, porém este regulamento trata sobre o tratamento de dados pessoais de prestação de serviços de comunicações eletrônicas publicamente disponíveis nas redes públicas de comunicações da comunidade.

Este regulamento deixa claro em seu art. 4º e 5º os aspectos necessários de segurança e confidencialidade das comunicações respectivamente. Destaca-se que é mais uma regulamentação europeia que tem consonância com o Regulamento Geral de Proteção de Dados, portanto, deve ser observada no que concerne a necessidade factual do caso concreto.

Mesmo com este regulamento nº 2016/169 podendo ser utilizado, foi criado outro regulamento nº 2018/1725 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.° 45/2001 e a Decisão n.° 1247/2002/CE.

Este novo regulamento, mais recente, porém, não é impeditivo de utilização do regulamento 2016/169, deixando claro na sua exposição de motivos que:

> Uma abordagem coerente da proteção dos dados pessoais e a livre circulação dos mesmos na União implicam uma harmonização, tão ampla quanto possível, das regras de proteção de dados adotadas a nível das instituições, dos órgãos e dos organismos da União com as regras de proteção de dados adotadas para o sector público nos Estados- -Membros. Sempre que as disposições do presente regulamento sigam os mesmos princípios que as disposições do Regulamento (UE) 2016/679, de acordo com a jurisprudência do Tribunal de Justiça da União Europeia («Tribunal de Justiça»), esses dois conjuntos de disposições deverão ser interpretados de forma homogénea, sobretudo porque o regime do presente regulamento deverá ser entendido como equivalente ao regime do Regulamento (UE) 2016/679.

Assim, diante da análise do regulamento nº 2018/1725, observa-se plena consonância ao regulamento nº 2016/169, incluindo-se na verdade novas informações acerca, por exemplo, da confidencialidade das comunicações eletrônicas e da própria Autoridade Europeia de Proteção de Dados, que tem quase as mesmas atribuições e poderes das autoridades de controle, mas não são a mesma figura e trabalham em cooperação para efetivação da proteção de dados.

4. Federal Trade Comission - FTC e Federal Communications Comission - FCC

Ao trata-se desta situação nos Estados Unidos da América, seria um pouco diverso o procedimento devido ao sistema adotado neste continente acerca da criação de agências reguladoras.

Ocorre que, nos EUA somente após a grande depressão de 1929 iniciada com a quebra da bolsa de valores de Nova York, e logo em seguida com a implantação do Plano New Deal as agências reguladoras passaram a ter força neste continente. Nesse interim, o Presidente Franklin D. Roosevelt tinha o objetivo promover uma intervenção de ordem econômica, política e social para conseguir dirimir as alhas de mercado. O plano versava diversas medidas intervencionistas no continente norte-americano.

O intuito principal seria "especializar a atuação estatal (reconhecia-se ampla discricionariedade técnica e o controle judicial sobre os atos das agências era restrito) e neutralizar (ou amenizar) a influência política na regulação de setores sensíveis (através, v.g., da previsão de estabilidade aos dirigentes)" (OLIVEIRA, 2009, p.161)

Nesse sentido em 1946 foi promulgada a Lei de Procedimentos Administrativos[6], que dispunha da uniformização da decisão, em duas vertentes: a primeira o *rulemaking*, que seriam as normas gerais das agências e a segunda a *adjudication*, atos individualizados. Isso permitia que o cidadão norte-americano tivesse uma garantia maior quanto a ilegalidade de atos pelos tribunais, caso as agencias desobedecessem a esta lei (OLIVEIRA, 2009).

> A importância das agências reguladoras pode ser caracterizada tradicionalmente pelo elevado grau de independência em relação ao Executivo e aos demais Poderes. Nelas se concentravam competências típicas dos três poderes institucionalmente constituídos: administrativas (função de administrar interesses), "quase judiciais" (resolução de conflitos de interesses entre os entes regulados) e "quase legislativas" (poder para editar normas gerais) (OLIVEIRA, 2009, p.162).

[6] Adminstrative Procedure Act – APA. Tradução nossa.

Apesar da importância das agências reguladoras naquele momento, inúmeras críticas ao modelo independente das agências foram realizadas. Entre as maiores críticas, a mais significativa foi a baseada na "Teoria da Captura", que dissertava sobre "o risco de que a regulação fosse capturada pelos entes regulados para satisfazerem apenas os seus interesses privados"(OLIVEIRA, 2009, p.162).

Outras críticas baseadas na "Teoria Econômica da Regulação da Escola de Chicago", desenvolvida na década de 70 por George Stigler, que tangenciava para "o risco de que a regulação econômica servisse para a satisfação dos interesses privados dos grupos politicamente influentes"(OLIVEIRA, 2009, p.162).

Assim, na década de 70 inicia-se nos EUA um processo de desregulação da economia, o chamado, *desregulation*, em que o Estado diminuiu as restrições a vários setores econômicos, diminuindo a intervenção das agências reguladoras sobre os entes privados. Consequência disso foi a "a ampliação do controle exercido pelos poderes constituídos em relação aos atos das agências"(OLIVEIRA,2009, p. 163-164).

O controle do judiciário é ampliado através do *hard-look doutrine*, que garantia ao judiciário a avaliação da legalidade e razoabilidade das medidas regulatórias das agências. Já o controle do executivo é intensificado. Surge a figura do Escritório de Orçamento e Execução[7] que supervisiona as propostas orçamentarias, e o Escritório de Informação e Regulação[8], que é responsável pela adequação da política presidencial com a atuação das agências reguladoras.

Assim, foram surgindo diversas ordens executivas com o propósito de diminuir a autonomia das agências, como as ordens executivas nº 12.291, 12.498 e 12.886/93, emitidas nos governos Reagan e de Bill Clinton (OLIVEIRA, 2009).

Por fim, o controle parlamentar, ou seja, o controle pelo legislativo foi fortalecido com a necessidade de aprovação pelo Congresso, a partir de 1993, onde os projetos e atividades das agências deveriam ser votados. Existia assim, um controle prévio chamado *rules review* e um controle posterior chamado *legislative veto* (OLIVEIRA, 2009).

Nesse interim, para evitar uma estabilização forçada do procedimento regulatório, foi promulgada a Lei sobre Negociação de Regulamentos[9] em 1990, que garantia que os titulares que tivessem seus interesses afetados pelo regulamento pudessem participar de sua elaboração (OLIVEIRA, 2009).

[7] Office of Management and Budget – OMB. Tradução nossa.
[8] Office of Information and Regulation Affars – OIRA. Tradução nossa.
[9] Negotiated Rulemaking Act – NRA. Tradução nossa.

Em 1995, uma nova legislação foi criada pelo congresso para limitar a discricionariedade e aumentar o controle financeiro das agências reguladoras. A Lei de Reforma dos Mandatos não Financiados[10], em seu título II obrigava as agências reguladoras a apresentarem informações sobre o custo de suas políticas públicas e regulação, a pesquisar dados de outros órgãos antes de criarem qualquer regulação e também buscarem opções que diminuíssem os custos da regulação (GULLO, 2004).

Após isso, no governo de Barack Obama, as ordens executivas sofreram algumas modificações devido a crise imobiliária e do sistema financeiro em 2008, havendo duas modificações, uma em 2009, sendo a Ordem executiva nº 13.497 e outra em 2011, sendo ela a ordem executiva nº 13.563.

Por fim, o que se pode resumir é que mesmo com o fim do New Deal, as crises sofridas no governo norte-americano desde 2008 até os tempos atuais influenciam na política regulatória dos EUA. Não há possibilidade de voltar-se a um modelo totalmente independente das agências, por isso elas continuam sobre o controle dos outros poderes do estado como uma forma de garantir os interesses de forma genuína do povo norte-americano.

Assim, após todo esse esboço histórico, passamos então a falar de duas agências específicas, foco deste trabalho. A primeira é a FTC – Federal Trade Comission (Comissão Federal de Comércio), criada em 1914, logo no início das agencias reguladoras nos EUA. Essa agência foi criada a partir da transformação do Escritório de Corporações, que foi criado em 1903. Essa agência atua na regulação das concorrências e na fiscalização de possíveis condutas de concorrência desleal e abuso do poder econômico, uma agencia antitruste. Posteriormente a FTC ampliou seus poderes, passando a agir também na defesa dos consumidores.

Já a FCC, ou seja, Federal Communications Comission (Comissão Federal de Comunicações) foi criada no período de criação do New Deal, em 1934, com o intuito de regular o setor de telecomunicações. Atualmente ela atua sobre os direitos de comunicação, regulação e inovação tecnológica.

Essas duas agências atuam hoje dentro da inovação tecnológica, claro, dentro de seus crivos originais. No caso de uma mega vazamento de dados, como ocorreu no Brasil, recentemente, já citado em tópico anterior, seria da competência de ambas lidar com este mega vazamento. Mas como essas agências tratariam disto?

Inicialmente cumpre se falar do vazamento de dados de mais de 145 milhões de norte-americanos que tiveram seus dados vazados pela empresa Equifax, que realizou um

[10] Unfunded Mandates Reform Act – UMRA. Tradução nossa.

acordo com a FTC aceitando pagar até US$ 1,4 bilhões de dólares por sua responsabilidade no vazamento de dados.

O primeiro vazamento de dados o Brasil, foi legitimamente maior que este vazamento nos EUA. No Brasil, ainda não há informação contundente de quem haveria sofrido a falha que gerou o vazamento de dados iniciais, porém, especula-se que tenha sido através da empresa Serasa Experian.

Quando falamos de vazamento de dados nos EUA, necessita-se falar no caso Equifax, caso este memorável, pois foi o primeiro caso de reembolso as vítimas do vazamento de dados e que criou uma jurisprudência para os casos futuros.

No caso Equifax, o acordo celebrado no Tribunal do Distrito de Atlanta, inclui um comprometimento da empresa em investir pelo menos US$ 1 bilhão de dólares em sistemas de segurança eletrônica para os servidores durante os próximos 05 anos. Inclui também a criação de um fundo inicial de US$380,5 milhões de dólares para o pagamento de serviços de monitoração de crédito e assistência financeira para clientes vítimas de fraude devido as informações vazadas, além de despesas das vítimas para recuperar suas informações e resolução de violações por roubo de identidade após a confirmação do vazamento pela Equifax.

Fora tudo isso a Equifax adicionou o importe de US$ 125 milhões de dólares, para caso o valor já alocado não seja suficiente para resolver os problemas das vítimas e disponibilizou até US$ 2 bilhões caso todos os 147 milhões de consumidores vítimas do vazamento se cadastrem para receber as indenizações, o que faria o valor real do acordo subir de US$ 1,4 bilhões de dólares para US$ 3 bilhões.

Para cada um dos consumidores cadastrados para receberem a indenização a Equifax terá que pagar US$ 25 (vinte e cinco dólares) para as horas usadas realizando medidas preventivas para identidades que poderiam ser roubadas ou recuperação de identidades roubadas; um reembolso de US$ 20 mil dólares por perda de documentos devido ao vazamento, que incluem o congelamento ou descongelamento de crédito, contratação de serviços de monitoramento de crédito, perdas financeiras pelo roubo de identidades vazadas ou qualquer outro tipo de fraude com fundo de dados vazados em 2017.

Também terá que pagar um reembolso de 25% do valor pago para os clientes que haviam contratado o serviço de monitoramento de crédito da Equifax no período de até 01 (um) ano antes do vazamento, ou seja, em 2016. Pagará 04 anos de serviços de monitoramento de crédito e proteção de identidades que será um serviço fornecido pela empresa Experian. Além deste serviço pago à Experian, depois será pago aos consumidores mais 06 anos de serviço de

monitoramento fornecido então pela Equifax, com compensação de US$ 125 (cento e vinte e cinco dólares) para quem já possui este tipo de serviço.

Por fim, a Equifax também terá que pagar aos consumidores um serviço de recuperação de identidade fornecido pela Experian para todos que foram vítimas de fraudes por conta do vazamento de dados em 2017, que será ofertado pelos próximos 07 anos. Estes eram os pontos cruciais do acordo. Acordo este que foi muito viável aos consumidores e serviu como base jurisprudencial para os próximos casos.

Assim, diante destes desdobramentos, podemos ver uma atuação insidiosa da FTC sobre o caso diante da proteção dos consumidores, situação está não tão evidenciada no Brasil, pois a ANPD sozinha ainda não conseguiu dinamizar um procedimento para solucionar a lesão aos consumidores neste caso. Na tentativa de resolução de grandes vazamentos anteriores a ANPD em conjunto com a Policia Federal tem tentado investigar o início desses vazamentos.

Enquanto isso, o Procon/SP tem agido com mais celeridade, indo atrás no caso ao qual eles já tem acesso a base de dados violada que foi a das empresas de telefonia, Claro, Oi, Vivo e Tim, no Brasil.

Comparando este caso a uma possível violação desta repercussão nos EUA, obviamente a base de um novo acordo seria este acordo da Equifax, só que agora inserindo além da FTC, a FCC, pois trata-se de um problema nas redes de telecomunicações. Enquanto a FTC trabalha com a violação de dados de maneira mais genérica e proteção ao consumidor a FCC trabalha diretamente com a violação de dados dentro das telecomunicações.

Obviamente, em conjunto as duas poderiam tratar sobre o assunto, garantindo ao cidadão norte-americano uma maior segurança.

O que se pode observar de mais diferente entre as indenizações das agências reguladoras norte-americanas e brasileira são os valores das indenizações, que nos EUA possuem valores de fato extremos, garantindo o papel da punição, seguindo a doutrina do *punitive damages*[11] adotada pelo ordenamento jurídico estadunidense (GEISTFELD, 2011).

Enquanto isso, no Brasil as punições podem chegar ao máximo a R$50 milhões de reais que não chegam a sequer reparar os danos sofridos pelas vítimas. Porém, a ANPD só poderá se valer da LGPD a partir de agosto de 2021. O que se observa, portanto, é uma doutrina composta pelo *Common Law* um pouco mais punitiva, porém que observa melhor o caso

[11] No caso Cole v. Tucker, o tribunal do Texas diferenciou os danos compensatórios (compensatory damages), que tem uma função compensatória, e os danos punitivos (punitive damages), sendo este sempre caracterizado quando o lesado estiver sendo alvo de uma conduta ilícita, objetivando a punição do agente do ilícito e reprimindo a repetição da conduta por ele.

concreto que no Brasil, que adota o *Civil Law*, ficando preso as determinações legais, que não avaliam por completo o caso concreto e o dano sofrido de forma específica pela taxação de valores prévia.

5. Conclusão

Diante de casos de vazamento de dados de companhias telefônicas, como ocorreu no Brasil, espera-se agora na ANPD uma maior interação acerca do seu papel e da sua competência. O estudo comparado das agências reguladoras europeias e note americanas traz uma perspectiva muito mais ativa das agências.

Na Europa, observa-se uma evolução enorme sobre tudo aquilo de que se trata sobre a violação de dados pessoais, estando a frente legalmente, seja do Brasil, seja dos EUA. Já nos EUA, observa-se uma evolução acerca do tratamento indenizatório, onde apesar de eles não possuírem leis concretas que determinem como se daria a responsabilização, ou que deem a independência completa das agências reguladoras, elas ainda sim conseguem agir de forma a garantir ao consumidor sua proteção e uma reparação acerca de um problema de vazamento de dados.

O que se pode concluir é que falta no Brasil, não a legislação de proteção de dados, que já temos e que se respalda muito bem na legislação europeia, mas claro, que necessita de alguns reparos. Falta no Brasil uma melhor atuação da ANPD, pois mesmo que o SENACON, ou o próprio Procon/SP, ou a Polícia Federal, possam trabalhar conjuntamente com a agencia, no Brasil existe regulamentação para o papel das agências reguladoras nestes casos, mesmo que ela só possa começar agir a partir de agosto de 2021. Portanto, falta uma maior eficácia da ANPD e a urgente regulamentação interna da mesma assim como a regulamentação sobre como se agir em casos de incidentes de segurança, como os tratados neste artigo.

REFERÊNCIAS

BRASIL. **Lei nº 13790 de 14 de agosto de 2018**. Lei Geral de proteção de Dados (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 20/02/2021.

BRASIL. **Nota Técnica nº 3/2021/CGN/ANPD**. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-imagens/sei_00261-000098_2021_67-nt-ts-incidente.pdf. Acesso em: 05/03/2021.(a)

BRASIL. **Portaria nº 21 de 27 de janeiro de 2021**.Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313. Acesso em: 05/03/2021.(b)

DOHMANN, Indra Spiecker Gen. **A proteção de dados pessoais sob o regulamento geral de proteção da dados da União Europeia**. DONEDA, Danilo. Et. Al. In: Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021.

GEISTFELD, Mark A. Due process and the deterrence rationale for punitive damages. **New York University Public Law and Legal Theory Working Papers**. Paper 311. 2011. Disponível em: https://lsr.nellco.org/nyu_plltwp/311. Acesso em: 20/01/2021.

GULLO, Theresa. History and Evaluation of the Unfunded Mandates Reform Act. **National Tax Journal**. Vol. LVII, nº 3, set. 2004. p. 559-570. Disponível em: https://www.journals.uchicago.edu/doi/pdf/10.17310/ntj.2004.3.04. Acesso em: 20/01/2021.

OLIVEIRA, Rafael de Carvalho Rezende de. O Modelo Norte-Americano de Agências Reguladoras e sua Recepção pelo Direito Brasileiro. **Revista EMERJ**. v. 12. n. 47. 2009.p.161. Disponível em: https://core.ac.uk/download/pdf/16041889.pdf. Acesso em: 20/02/2021

UNIÃO EUROPEIA**. Directiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de Julho de 2002**. Relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas). Disponível em: https://edps.europa.eu/sites/edp/files/publication/dir_2002_58_pt.pdf. Acesso em: 20/02/2021.

UNIÃO EUROPEIA. **European Data Protection Supervisor (EDPS)**. Disponível em: https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_en. Acesso em: 21/02/2021.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/ 679 do Parlamento Europeu e do Conselho de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/ 46/ CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Acesso em: 20/01/2021.

UNIÃO EUROPEIA. **Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018**. Relativo à proteção das pessoas singulares no que diz

respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.° 45/2001 e a Decisão n.° 1247/2002/CET exto relevante para efeitos do EEE. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32018R1725&from=EN. Acesso em: 20/02/2021.

USA. **Federal Communications Commission | The United States of America**. Disponível em: https://www.fcc.gov/. Acesso em 21/02/2021.

USA. **Federal Trade Comission**. About the Federal Trade Comission. Disponível em <http://www.ftc.gov/ftc/about.shtm>. Acesso em 21/02/2021.

USA. **Office of Information and Regulatory Affairs (EUA)**. Executive Order 12866 Regulatory Planning and Review. Disponível em <http://www.reginfo.gov/public/jsp/Utilities/EO_Redirect.jsp>. Acesso em 20/02/2021.

USA. **Case No. 1:17-md-2800-TWT (N.D. Ga)**. Settlement Agreement And Release made as of May 15, 2020, by and between, as hereinafter defined, (a) Settlement Class Representatives on behalf of themselves and the Settlement Class, (b) the Association Plaintiffs, and (c) Equifax Inc. and Equifax Information Services LLC (collectively, “Equifax” or “Defendants”) and subject to preliminary and final Court approval as required by Rule 23 of the Federal Rules of Civil Procedure. Disponível em: https://pacer.login.uscourts.gov/csologin/login.jsf?pscCourtId=GANDC&appurl=https://ecf.gand.uscourts.gov/cgi-bin/iqquerymenu.pl?244824. Acesso em: 20/01/2021.