PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO E RELAÇÕES INTERNACIONAIS
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
MONOGRAFIA JURÍDICA

AS SANÇÕES ADMINISTRATIVAS DA LGPD, RESPONSABILIDADE E RESSARCIMENTO DE DANOS: UMA ÓTICA A PARTIR DA VIOLAÇÃO AOS DADOS PESSOAIS PELO COMPARTILHAMENTO IRREGULAR E FALTA DE SEGURANÇA DA INFORMAÇÃO

ORIENTANDO - JOSÉ LUCAS DA COSTA DIAS
ORIENTADORA – PROF.ª DR.ª FERNANDA DE PAULA FERREIRA
MOI

GOIÂNIA-GO
2021

JOSÉ LUCAS DA COSTA DIAS

AS SANÇÕES ADMINISTRATIVAS DA LGPD, RESPONSABILIDADE E RESSARCIMENTO DE DANOS: UMA ÓTICA A PARTIR DA VIOLAÇÃO AOS DADOS PESSOAIS PELO COMPARTILHAMENTO IRREGULAR E FALTA DE SEGURANÇA DA INFORMAÇÃO

Monografia Jurídica apresentada à disciplina Trabalho de Curso II, da Escola de Direito e Relações Internacionais, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).
Prof.ª Orientadorª – Dr.ª Fernanda de Paula Ferreira Moi

GOIÂNIA-GO
2021

JOSÉ LUCAS DA COSTA DIAS

AS SANÇÕES ADMINISTRATIVAS DA LGPD, RESPONSABILIDADE E RESSARCIMENTO DE DANOS: UMA ÓTICA A PARTIR DA VIOLAÇÃO AOS DADOS PESSOAIS PELO COMPARTILHAMENTO IRREGULAR E FALTA DE SEGURANÇA DA INFORMAÇÃO

Data da Defesa: 07 de junho de 2021

BANCA EXAMINADORA

_____

Orientadora: Prof.ª Dr.ª Fernanda de Paula Ferreira Moi Nota

_____

Examinadora Convidada: Prof.ª M.ª Ana Flávia Mori L. C. Rosa Nota

Dedicatória

Dedico esta monografia à minha família, que nos momentos mais difíceis de minha vida não mediram esforços para me proporcionar as melhores condições de estudo, e pelo amor e apoio incondicional.

Agradecimentos

Agradeço a Deus por tudo que tem me proporcionado. À minha família, pelo exemplo de força e superação. À minha namorada, Helouyse Dantas, pela compreensão e apoio. À inspiradora, dedicada e respeitosa orientadora Fernanda Moi, com eterna gratidão. E a todos que estão ao meu lado nessa caminhada chamada vida.

SUMÁRIO

RESUMO

A presente monografia tem como objetivo analisar a aplicabilidade da Lei Geral de Proteção de Dados através da instrumentalização jurídica de suas sanções pelo Estado, fazendo um cotejo indispensável com outras normas do direito brasileiro, imprescindíveis para a exposição e explanação deste trabalho. No desenvolvimento da pesquisa pretende-se solucionar a seguinte questão investigativa: Em um dos países mais propenso a sofrer vazamentos de dados em todo o mundo, os nossos dados pessoais estão seguros diante da LGPD e suas sanções?. A estruturação da monografia se baseará na utilização do método hermenêutico através de uma perspectiva teleológica/axiológica do ordenamento jurídico aplicável da LGPD em relação às suas sanções. Assim, a metodologia a ser empregada para a aplicação do método apresentado, consistirá em revisão bibliográfica, bem como estudos de casos que apresentem o emprego da LGPD, suas sanções e outras responsabilidades, com a finalidade de criar um cotejo indispensável entre a teoria e a realidade. Logo, infere-se que ao analisar as sanções da LGPD à luz dos pressupostos metodológicos aqui expostos nos conduz a uma interpretação mais abrangente, que é de fundamental importância para a sua aplicabilidade.

PALAVRAS-CHAVE: LGPD; vazamentos de dados; sanções; responsabilidades; aplicabilidade.

INTRODUÇÃO

Tendo em vista a crescente exposição da sociedade que a tecnologia da informação gera, frequentemente acontecem diversos casos de violação de dados pessoais e de vazamentos de informações, expondo dados e informações confidenciais dos titulares. Assim, torna-se imprescindível uma regulamentação que propicie a proteção de dados e a aplicação de sanções para com os infratores.

O presente trabalho tem como objetivo analisar a aplicabilidade da Lei Geral de Proteção de Dados através da instrumentalização jurídica de suas sanções pelo Estado, fazendo um cotejo indispensável com outras normas do direito brasileiro, imprescindíveis para a exposição e explanação desta monografia.

Desta forma, visa apresentar as sanções administrativas, responsabilidade e ressarcimento de danos a partir da violação aos dados pessoais pelo compartilhamento irregular e falta de segurança da informação analisando conforme a obra de Helen Nissenbaum, 2010, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* [1](Inglês), que demonstra a necessidade de um contexto que enfatiza a maleabilidade da privacidade de acordo com o cenário, contextos nos quais cada vigilância, por exemplo as realizadas por câmera, podem ser pensadas como aceitáveis, ou o contrário.

Neste viés, o compartilhamento de dados de uma compra sem o consentimento do titular estão fora dos limites, ao passo que a instalação de câmeras em sinais de trânsito muitas vezes são consideradas legítimas.

Assim sendo, cabe aqui ressaltar que a exposição e coleta de dados na internet deve ser contextual, conforme a teoria da integridade contextual (*contextual integrity*) formulada pela professora de ciência da informação Helen Nissenbaum.

No desenvolvimento da pesquisa pretende-se solucionar a seguinte questão investigativa: Em um dos países mais propenso a sofrer vazamentos de dados em todo o mundo, os nossos dados pessoais estão seguros diante da LGPD e suas sanções?

A estruturação da monografia se baseará na utilização do método hermenêutico através de uma perspectiva teleológica/axiológica do ordenamento

[1]Privacidade em contexto: tecnologia, política e integridade da vida social.

jurídico aplicável da LGPD em relação às suas sanções. Entende-se por hermenêutica o conjunto de técnicas que possibilitam ao intérprete obter a ampla compreensão de um texto, levando-o a atribuir determinados significados ao que está escrito.

Ao adotar o método teleológico ou finalista que consiste na busca da finalidade da norma, procurará, assim, superando a realidade escrita da lei, a compreensão da norma através da razão finalística que motivou a produção normativa.

Posto isso, infere-se que ao analisar as sanções da LGPD à luz dos pressupostos metodológicos aqui expostos nos conduz a uma interpretação mais abrangente, que é de fundamental importância para a sua aplicabilidade. Assim, é possível perceber que tal método se adequa ao tema em questão, uma vez que, será feita uma análise aprofundada que busca a compreensão da realidade brasileira em relação à coleta e armazenamento de dados, como as normas que o regulam.

Enfim, a metodologia a ser empregada para a aplicação do método apresentado, consistirá em revisão bibliográfica, bem como estudos de casos que apresentem o emprego da LGPD, suas sanções e outras responsabilidades, com a finalidade de criar um cotejo indispensável entre a teoria e a realidade.

O trabalho foi dividido em três capítulos elaborados com base em materiais coletados em pesquisas, relatórios, notícias, livros, doutrinas, artigos científicos e legislação nacional e estrangeira sobre o tema. O primeiro capítulo desse trabalho procura esclarecer a respeito do direito à privacidade e tratamento de dados na legislação brasileira, ou seja, apresenta o Direito Constitucional à privacidade previsto na Constituição da República Federativa do Brasil, bem como as leis infraconstitucionais que regem o direito digital e a Lei Geral de Proteção de Dados (LGPD), enfoque desse trabalho.

Logo depois, o segundo capítulo tratará especificamente da violação de dados no Brasil demonstrando a exposição do internauta na *web* e a coleta de seus dados, da qual faz uma elucidação indispensável da falta de segurança da informação e compartilhamento irregular desses dados coletados.

Por fim, o terceiro capítulo fará o desfecho expondo casos brasileiros de violação aos dados pessoais pelo compartilhamento irregular e falta de segurança da informação por intermédio do ordenamento jurídico vigente, como também a contextualização das sanções aplicadas.

CAPÍTULO I - DIREITO À PRIVACIDADE E TRATAMENTO DE DADOS NA LEGISLAÇÃO BRASILEIRA

1.1 DIREITO CONSTITUCIONAL À PRIVACIDADE

A privacidade tem o seu conceito a partir de origens históricas em discussões filosóficas bem conhecidas, mais notavelmente a distinção feita por Aristóteles entre a esfera pública da atividade política (*polis*) e a esfera privada associada à família e à vida doméstica (*oiko*), "[...] como duas esferas distintas da vida, é uma referência clássica a um domínio privado" (Tradução livre) (DECEW, 2018).

Uma discussão escrita mais sistemática do conceito de privacidade teve-se início com o famoso ensaio de Samuel Warren e Louis Brandeis intitulado "*The Right to Privacy*" (Inglês)[2]. Citando "mudanças políticas, sociais e econômicas" e um reconhecimento do "direito de ser deixado em paz" (WARREN, S.D., BRANDEIS, L.D., 1890, p. 193), eles argumentaram que a lei existente oferecia uma maneira de proteger a privacidade do indivíduo e procuraram explicar a natureza e a extensão dessa proteção.

Warren e Brandeis enfatizaram a invasão de privacidade provocada pela divulgação pública de detalhes relativos à vida privada de uma pessoa, perceberam que uma variedade de casos existentes poderiam ser protegidos por um direito mais geral à privacidade, que protegeria até que ponto os pensamentos, sentimentos e emoções de alguém poderiam ser compartilhados com outras pessoas. Com uma vontade de alcançar uma paz de espírito com tal proteção, eles disseram que o direito à privacidade era baseado em um princípio de "personalidade inviolável" e "como parte do direito mais geral à imunidade da pessoa, - o direito à própria personalidade." (Tradução livre) (WARREN, S.D., BRANDEIS, L.D., 1890, p. 207).

Ao longo do tempo, o *right of privacy*, desenvolvido como um conceito da *common law*, ou seja, a partir de decisões dos tribunais, e não mediante atos legislativos ou executivos, passou a aparecer em casos envolvendo a Constituição dos Estados Unidos da América. Todavia, apesar de o início dos debates ter ocorrido ainda na primeira metade do século XX, o reconhecimento do *right of privacy* na

[2]O Direito à privacidade

Constituição somente veio com o caso Griswold *v.* Connecticut, decidido em 1965 pela Suprema Corte dos Estados Unidos (RIGAUX, 1990, p. 167, *apud* ZANINI, 2015, p. 305).

Na demanda, foi debatida uma lei de Connecticut que tornou ilegal o uso ou a distribuição de anticoncepcionais, o que configuraria ingerência do Estado no *privacy*. A lei deu causa à condenação de um médico que examinou uma mulher casada e prescreveu métodos contraceptivos, bem como do senhor Griswold, diretor da clínica onde o referido médico trabalhava (ZANINI, 2015, p. 303).

Na Suprema Corte dos Estados Unidos, o juiz William Douglas redigiu o voto do caso Griswold *v.* Connecticut, que se tornou célebre. Nele, o magistrado declarou a inconstitucionalidade da lei e reconheceu a existência de um direito geral de *privacy*, que decorreria das seguintes emendas à Constituição dos Estados Unidos: primeira (liberdade de expressão), terceira (restrição ao aquartelamento de soldados em casas particulares), quarta (buscas e apreensões ilícitas), quinta (autoincriminação) e nona (declara que os direitos não especificados na Declaração de Direitos são também protegidos por ela) (ZANINI, 2015, p. 306).

A decisão ainda destaca o caráter sacro da união conjugal e o respeito que merece a intimidade do casal, considerando, por conseguinte, inadmissível que a polícia pudesse estender suas investigações ao quarto do casal ("*the sacred precincts of marital bedrooms*") (RIGAUX, 1990, p. 167, *apud* ZANINI, 2015, p. 306).

Dessa maneira, somente a partir do caso Griswold *v.* Connecticut é que vai ser reconhecido constitucionalmente, pela primeira vez, o *right of privacy*, que, apesar de não ser expressamente mencionado pela Constituição, estaria localizado, conforme o voto do juiz Douglas, no interior das liberdades criadas por uma interpretação mais abrangente da declaração de direitos (SOLOVE, ROTENBERG, SCHWARTZ, p. 28-29, *apud* ZANINI, 2015, p. 306).

Desta forma, cabe destacar um trecho do parecer emitido pelo Juiz William Orville Douglas na época:

> (...) Várias garantias criam zonas de privacidade. O direito de associação contido na penumbra da Primeira Emenda é um, como vimos. A Terceira Emenda, em sua proibição do aquartelamento de soldados "em qualquer casa" em tempo de paz, sem o consentimento do proprietário, é outra faceta dessa privacidade. A Quarta Emenda afirma explicitamente o "direito das pessoas de estarem seguras em suas pessoas, casas, papéis e pertences, contra buscas e apreensões irracionais". A Quinta Emenda em sua Cláusula

> de Autoincriminação permite ao cidadão criar uma zona de privacidade que o governo não pode obrigá-lo a ceder em seu detrimento. A Nona Emenda dispõe: "A enumeração na Constituição, de certos direitos, não deve ser interpretada para negar ou menosprezar outros retidos pelo povo."(...)
> Tivemos muitas controvérsias sobre esses direitos penumbrais de "privacidade e tranquilidade". Esses casos testemunham que o direito à privacidade que aqui exige reconhecimento é legítimo. (...)
> O presente caso, portanto, diz respeito a uma relação inserida na zona de privacidade criada por várias garantias constitucionais fundamentais. E trata-se de uma lei que, ao proibir o uso de anticoncepcionais em vez de regulamentar sua fabricação ou venda, busca atingir seus objetivos por meio de um impacto destrutivo máximo sobre essa relação. Tal lei não pode permanecer à luz do princípio familiar, tão frequentemente aplicado por este Tribunal, de que um “propósito governamental de controlar ou prevenir atividades constitucionalmente sujeitas à regulação estatal não pode ser alcançado por meios que varrem desnecessariamente de forma ampla e, assim, invadem a área de liberdades protegidas”. (...)
> Lidamos com um direito à privacidade mais antigo do que a Declaração de Direitos - mais antigo do que nossos partidos políticos, mais antigo do que nosso sistema escolar. O casamento é uma união para o melhor ou para o pior, esperançosamente duradouro e íntimo ao grau de ser sagrado. É uma associação que promove um modo de vida, não causas; uma harmonia na vida, não nas crenças políticas; uma lealdade bilateral, não projetos comerciais ou sociais. No entanto, é uma associação com um propósito tão nobre quanto qualquer outra envolvida em nossas decisões anteriores. (Tradução livre) (Griswold v. Connecticut, 381 US 479 - Supreme Court 1965)

Enquanto no Brasil, na Constituição de 1934 nasce, em nível constitucional, a expressão “Direitos e Garantias Individuais”, mantendo a inviolabilidade do sigilo de correspondência, a casa como asilo inviolável, bem como às obras literárias, artística e científicas (COLOMBO, 2017). Trata-se de Carta que se compromissa com três correntes de pensamento: os liberais de 1891; os defensores das ideias sociais, como a Constituição de Weimar, de 1919, vinculada ao constitucionalismo social; e uma corrente com viés corporativa e autoritário que se volta à representação profissional de classes econômicas (SOUZA JÚNIOR, 2002b, p. 47 *apud* COLOMBO, 2017).

Na Constituição de 1937, do Estado Novo, dada sua característica autoritária, os direitos se reduzem à “inviolabilidade do domicílio e da correspondência, salvas as excepções expressas em lei”. Não há mais no texto que a “casa é o asilo inviolável”, demonstrando real retrocesso na área da intimidade e vida privada. Uma curiosidade é que a referida Carta não fazia também menção ao termo “democracia” (SOUZA JÚNIOR, op. cit., p. 53 *apud* COLOMBO, 2017).

Apesar disso, a Constituição de 1946 retorna a tratar a casa como asilo inviolável (COLOMBO, 2017) em seu art. 141, § 15, não podendo penetrá-la à noite, sem consentimento do morador, fazendo-se uma retomada de direitos constitucionalmente garantidos.

Em 1955, Pontes de Miranda publica o volume 7 do Tratado de Direito Privado, abordando a temática dos “Direitos de Personalidade”, advertindo que, em pleno século XX, “juristas de prol resistiram a tratar a integridade psíquica, a honra e, até a liberdade de pensamento como direitos.” (MIRANDA, PONTES DE, 1955, p. 5 *apud* COLOMBO, 2017).

Transcorrido doze anos desta declaração, a Constituição de 1967 trouxe a novidade de que o sigilo de correspondência se estendia também às comunicações telegráficas e telefônicas (art. 150, § 9º). O que foi mantido na Emenda Constitucional de 1969. De tal arte, estes são os antecedentes históricos à Constituição Federal de 1988 (COLOMBO, 2017) sobre o direito de privacidade no Brasil.

A magna carta de 1988, em seu art. 5º, inciso X, tratou de proteger parte da privacidade, declarando que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação.

Segundo Dirley da Cunha Júnior (2018, p. 626):

> Direito à privacidade, tomada essa expressão em sentido amplo para abranger todas as manifestações da esfera íntima, privada e da personalidade das pessoas.

Neste sentido, a privacidade refere-se ao conjunto de informações a respeito do indivíduo, podendo ele decidir mantê-lo sob exclusivo controle seu, ou mesmo comunicar, escolhendo a quem, quando, ou sob quais condições, sem a isso poder ser sujeito em termos legais (SILVA, 1997, p. 209). Pode-se verificar que a esfera de inviolabilidade é bastante ampla e, conforme Moacyr de Oliveira (2001, p. 209), “abrange o modo de vida doméstico, nas relações familiares e afetivas em geral, fatos, hábitos, local, nome, imagem, pensamentos, segredos, e, bem assim, as origens e planos futuros do indivíduo.”.

Impende salientar que, em virtude da utilização de uma tecnologia bastante sofisticada, as pessoas ficam submetidas à vulnerabilidade de sua privacidade.

No entendimento de Kildare Gonçalves Carvalho (2009, p. 752):

> (...) o direito de estar só e o direito à própria imagem, às vezes tão impiedosamente exposta pelos meios de comunicação de massa, ganham eminência constitucional, protegendo-se o homem na sua intimidade e privacidade. O dano moral decorrente da violação desses direitos, além do dano material, será indenizado, encerrando assim a Constituição a polêmica até então existente no Direito brasileiro sobre a indenização do dano moral.

No panorama do ordenamento brasileiro, o reconhecimento da proteção de dados como um direito autônomo e fundamental não deriva de uma dicção explícita e literal, porém da consideração dos riscos que o tratamento automatizado traz à proteção da personalidade à luz das garantias constitucionais de igualdade substancial, liberdade e dignidade da pessoa humana, juntamente com a proteção da intimidade e da vida privada (DONEDA, 2011, p. 103).

O esforço a ser empreendido pela doutrina e pela jurisprudência seria, em nosso ponto de vista, basicamente o favorecimento de uma interpretação dos incisos X e XII do art. 5º mais fiel ao nosso tempo, ou seja, reconhecendo a íntima ligação que passam a ostentar os direitos relacionados à privacidade e à comunicação de dados. Desta forma, seria dado o passo necessário à integração da personalidade em sua acepção mais completa na vicissitudes da Sociedade da Informação (DONEDA, 2011, p. 106).

Destarte, o direito à privacidade da qual apresenta a nossa Constituição Federal só foi solidamente reconhecido através do julgamento da ADI 6387/DF em que o Supremo Tribunal Federal (STF) reconheceu que esse direito à privacidade decorre dos direitos da personalidade como liberdade individual, da privacidade e do livre desenvolvimento da personalidade segundo a ementa do acórdão:

> MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. REFERENDO. MEDIDA PROVISÓRIA Nº 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO NOVO CORONAVÍRUS (COVID-19). COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. FUMUS BONI JURIS. PERICULUM IN MORA. DEFERIMENTO. 1. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais. 2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados. (...) (ADI 6387/DF, Relatora Ministra Rosa Weber, Tribunal Pleno, julgado em 07/05/2020).

Desta forma, o acórdão modela a forma como se deve integrar e exteriorizar o direito à privacidade no Brasil, sendo fundamental sua interpretação e expansão conforme a legislação especial que toma a regra constitucional como norte, base e faz dela suas entranhas.

1.2 LGPD E LEIS INFRACONSTITUCIONAIS QUE REGEM O DIREITO DIGITAL

Em um mundo online abrangente, no ambiente virtual fornecido para comunicação na Internet por meio de mecanismos de busca e redes sociais (como Google e Facebook), a real liberdade de escolha dos conteúdos acessados pode representar, na verdade, um espaço de influência desses ambientes sobre os indivíduos, e não o contrário.

Maciej Cegłowski em seu artigo "*The New Wilderness*" para o *blog Idle Words*, postula que:

> Nenhuma outra empresa fez mais para arrastar a vida privada para o olho algorítmico do que Google e Facebook. Juntos, eles controlam a mais sofisticada operação de vigilância em "atacado" do mundo, um duopólio que gera quase dois terços do dinheiro gasto em anúncios online. (Tradução livre)

Isso ocorre porque, como indica Goulart (2014, p. 95) essa relação é formada por "uma série de algoritmos que selecionam o que é apresentado aos usuários".

Ao cruzar dados pessoais, essas plataformas criam um perfil de usuário, para que assim cada um receba resultados personalizados em suas pesquisas a partir de uma série de informações previamente identificadas. Essa é apenas uma pequena parte do poderoso controle que essas empresas de tecnologia podem exercer sobre seus usuários.

Assim, assevera Goulart (2014, p. 95):

> Por meio do intenso cruzamento e processamento de dados pessoais criam-se perfis de cada um dos usuários, em uma atividade chamada de *profiling*. Com isso, cada tipo de perfil receberá resultados personalizados que levam em conta uma série de aspectos identificados. Com tais informações, além do conteúdo ser personalizado, há também a personalização da propaganda.

Assim sendo, quando se trata de questões do ambiente virtual, o dilema entre segurança e privacidade deve ser amplamente discutido e embasado na lei vigente. Este ambiente possui tantas informações privilegiadas sobre cada consumidor, que favorece o consumo online, sobretudo com diversas facilidades disponibilizadas pelos

meios de *e-commerce*, para que os clientes possam encontrar de tudo a qualquer hora e em qualquer lugar.

Devido às poderosas funções de penetração da Internet, que bombardeia e reduz a escolha do consumidor, a publicidade está se utilizando dos recursos tecnológicos para se tornar onipresente.

Ante essa perspectiva Doneda (2010, p. 69) endossa:

> A necessidade de garantir os direitos do consumidor neste ambiente contra práticas abusivas, bem como de lhe proporcionar a efetiva proteção sobre suas próprias informações pessoais vem sendo, portanto, tema de iniciativas regulatórias em aspectos como, entre outros, a garantia do consentimento livre do consumidor para a atuação destes serviços, a salvaguarda de sua privacidade, a transparência desta atividade e a possibilidade de recusar-se a continuar recebendo publicidade comportamental, entre outros.

Por estes motivos delineados, tornou-se necessário regular o ambiente virtual, que agora está disciplinado pelo Marco Civil da Internet assimilando as mudanças sociais rápidas e profundas, pois o Direito deve compreender as mudanças nas estruturas da sociedade, no sentido individualizante, através de modelos flexíveis de regulação (CANOTILHO, 2003 *apud* FERREIRA; FERREIRA; DO CARMO, 2015).

Diante das demandas da sociedade por respostas jurídicas às investidas criminosas na internet, diversos países elaboraram leis para regulamentar e punir os crimes e abusos praticados nessa área, como a disseminação de vírus, transações bancárias ilegais, pedofilia etc. (FERREIRA; FERREIRA; DO CARMO, 2015).

A própria União Europeia passou a discutir lei que endurece regras sobre privacidade de dados, alterando a maneira como as empresas estrangeiras, principalmente as americanas, lidam com os dados do consumidor na Europa. Os usuários de sites e serviços como Twitter, Google e Facebook, conforme discussão de novo projeto de lei europeu, terão de consentir explicitamente para que as empresas possam compartilhar seus dados pessoais, obrigando a remoção de links com informações pessoais excessivas ou irrelevantes dos resultados dos mecanismos de busca na internet (TI INSIDE ONLINE *apud* FLORENÇO, 2016, p. 176).

Nesse sentido a Lei nº 12.965/2014, ou melhor, o Marco Civil da Internet foi o ato regulatório da rede mundial de computadores no Brasil que inicialmente

estabeleceu princípios, garantias, direitos e deveres para o uso da Internet[3]. Dando o pontapé inicial para a consolidação do direito digital no Brasil, pois, foi a primeira lei que cunhou a expressão literal “privacidade” no ordenamento jurídico pátrio, como exposto em seu art. 3º, inciso II, art. 8º e art. 11, § 3º:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> II - proteção da privacidade;
>
> Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.
>
> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
> § 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.

Por meio deste marco regulatório que trouxe em sua natureza proposições que visam à viabilidade ao disciplinamento do meio digital através do ordenamento pátrio, a referida lei se colocou com a finalidade de trazer segurança jurídica à sociedade brasileira dada a preocupação com a liberdade do acesso à informação e as mudanças nas relações sociais causadas pela internet.

Esse dispositivo legal assumiu o encargo de coibir a violação das garantias do serviço de rede e dos direitos dos usuários, como também sanar atritos e omissões nas políticas governamentais relacionadas à internet.

Através do Marco Civil da Internet, os serviços de comunicação de massa, por meio da rede mundial de computadores, mantêm sua característica original: a liberdade de iniciativa e a consequente formatação de novos modelos de negócios. Entretanto, sua atuação deve estar sempre orientada a respeitar os princípios legais e os limites estabelecidos, decorrentes das normas de defesa do consumidor, de proteção à criança e ao adolescente e de atenção às garantias constitucionais (FERREIRA; FERREIRA; DO CARMO, 2015).

---

[3] Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

Apesar disso, quando o Marco Civil da Internet trata de proteção de dados pessoais, comércio eletrônico, crimes cibernéticos, direitos autorais, governança da Internet e supervisão das atividades dos provedores de Internet, ele impõe a presença do Estado no ambiente virtual, dando ao poder público competência de atuação, garantindo e ordenando a universalidade e a diversidade ao acesso à internet para que esse seja, de fato, um meio de desenvolvimento social, de exercício da cidadania, promoção da cultura e desenvolvimento tecnológico (FERREIRA; FERREIRA; DO CARMO, 2015).

No entanto, para Eduardo Tomasevicius Filho o Marco Civil da Internet trouxe poucos aspectos positivos em razão da ingenuidade do legislador brasileiro de manter a pretensão de solucionar problemas de escala mundial, com efeitos extraterritoriais, por meio de uma lei nacional.

> Na tentativa de frear violações de privacidade por meio de coleta, armazenamento e tratamento de registros, dados pessoais ou comunicações, por meio do art.11, caput, §§1º e 2º, estabeleceu-se que o Marco Civil da Internet se aplica quando, pelo menos, um dos atos realizar-se no Brasil ou quando um dos terminais estiver no Brasil e que pessoas jurídicas com sede no exterior devem sujeitar-se à lei brasileira quando tiverem, pelo menos, uma integrante do mesmo grupo econômico com estabelecimento no Brasil. A despeito da boa intenção, a violação pode não acontecer no Brasil, mas poderá acontecer na outra ponta da transmissão de dados no exterior. (TOMASEVICIUS FILHO, 2016, p. 277)

Desta maneira, a proteção de dados pessoais e sensíveis no ordenamento pátrio só veio efetivamente através da vigência a partir de agosto de 2020 da Lei Geral de Proteção de Dados, Lei nº 13.709, regimento este atual e específico que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A lei criou uma situação de segurança jurídica por meio da padronização de normas e práticas para promover a proteção de forma igualitária e dentro do país e no mundo, aos dados pessoais de todo cidadão que esteja no Brasil.

Segundo Bruno Bioni (2020, p. 258):

> Uma lei que terá um impacto econômico-social e regulatório como poucas outras tiveram na história do país, suplantável ao que foi o Código de Defesa do Consumidor e a Consolidação das Leis Trabalhistas. (...) Em razão desse contexto, leis gerais de proteção de dados pessoais, como a Lei 13.709/2018,

> são elevadas, por vezes, ao patamar de um novo contrato social. Nelas se encontram as “regras do jogo” para o próprio funcionamento pacífico e democrático da sociedade.

Assim, a lei primeiro propôs o que são dados pessoais, definindo que há dados sujeitos a cuidados ainda mais específicos, como os sensíveis, os sobre crianças e adolescentes, e que dados tratados tanto nos meios físicos como digitais estão sujeitos à sua regulação (Seções I, II e III da LGPD).

Estabeleceu ainda que não importa se a sede de uma organização ou seu *data center* (centro de dados) está localizado no Brasil ou no exterior: se há o processamento de conteúdo de pessoas, brasileiras ou não, que estão no território nacional, a LGPD deve ser cumprida (art. 3º da LGPD).

Também determinou que é permitido compartilhar dados com organizações internacionais e outros países, desde que isso ocorra a partir de protocolos seguros e/ou para cumprir exigências legais (art. 33, inciso I da LGPD).

Outro elemento básico da LGPD é o consentimento. Por outras palavras, o consentimento dos cidadãos é a base para o tratamento dos dados pessoais. Se antes o fluxo das informações pessoais deveria ser autorizado pelo Estado, agora cabe ao próprio cidadão tal ingerência que, por meio do consentimento, estabelece as suas escolhas no tocante à coleta, uso e compartilhamento dos seus dados pessoais (BIONI, 2019, p. 115).

Mas há algumas exceções, os dados podem ser processados sem consentimento se for indispensável para: cumprir uma obrigação legal; executar política pública prevista em lei; realizar estudos via órgão de pesquisa; executar contratos; defender direitos em processo; preservar a vida e a integridade física de uma pessoa; tutelar ações feitas por profissionais das áreas da saúde ou sanitária; prevenir fraudes contra o titular; proteger o crédito; ou atender a um interesse legítimo, que não fira direitos fundamentais do cidadão (art. 11, inciso II da LGPD).

A disseminação de autoridades independentes para a aplicação das leis de proteção de dados pessoais, bem como de proposições normativas, que não deixavam ao reino do indivíduo a escolha sobre o processamento de certos tipos de dados pessoais, relativizaram a referenciada centralidade do consentimento. (BIONI, 2019, p.116-117).

Portanto, pode-se especular que o Estado perdeu seu monopólio do controle de dados para fornecer maior autonomia e protagonismo para outras entidades como empresas privadas e até mesmo para o indivíduo – detentor dos próprios dados pessoais.

Ademais, é essencial saber que a lei oferece uma série de garantias aos cidadãos, que podem solicitar a exclusão de dados, a revogação do consentimento, a transferência de dados para outro prestador de serviços, entre outras ações (art. 18 da LGPD).

Cabe salientar que o tratamento de dados deve levar em conta algumas questões, como a finalidade e necessidade, e essas questões devem ser previamente acordadas e informadas aos cidadãos (art. 9º da LGPD).

Nesse sentido, o artigo publicado pelo SERPRO intitulado “O que muda com a LGPD”, que busca elucidar pormenores da LGPD, demonstra:

> Por exemplo, se a finalidade de um tratamento, feito exclusivamente de modo automatizado, for construir um perfil (pessoal, profissional, de consumo, de crédito), o indivíduo deve ser informado de que pode intervir e pedir revisão desse procedimento feito por máquinas.

Necessário ressaltar que o país contará com a Autoridade Nacional de Proteção de Dados Pessoais, a ANPD. A instituição fiscalizará e aplicará penalidades se a LGPD for descumprida. Além disso, caberá a ANPD as tarefas de regular e de orientar, preventivamente, sobre como aplicar a lei. Ademais, os cidadãos e as organizações poderão cooperar com a autoridade.

No entanto, não basta a ANPD - que está em formação - razão pela qual a Lei Geral de Proteção de Dados Pessoais também estipula os agentes de tratamento de dados e suas funções[4], nas organizações: tem o controlador, que toma as decisões sobre o tratamento; o operador, que realiza o tratamento, em nome do controlador; e o encarregado, que interage com cidadãos e autoridade nacional (e poderá ou não ser exigido, a depender do tipo ou porte da organização e do volume de dados tratados).

Há outro item que não pode ser ignorado: gerenciamento de riscos e falhas. Isso significa que qualquer pessoa que gerencia um banco de dados pessoal deve

[4] Art. 5º, incisos VI, VII e VIII da Lei 13.709/2018.

escrever regras de governança, tomar medidas preventivas de segurança, copiando as boas práticas e certificações existentes no mercado. Terá ainda que elaborar planos de contingência; fazer auditorias; resolver incidentes com agilidade (art. 50 da LGPD).

Por exemplo, se ocorrer um vazamento de dados, a ANPD e os indivíduos afetados devem ser notificados imediatamente. Observa-se que há de se adaptar com rigoroso controle, os setores responsáveis pela coleta e ao tratamento de dados pessoais, criando ações específicas a fim de cumprir os requisitos da lei, implementando as novas regras, de acordo com as características de cada departamento (BIONI, 2019 *apud* AYRES, 2019). Vale lembrar que todos os agentes de tratamento estão sujeitos à legislação. Isso significa que as organizações e as subcontratadas para tratar dados respondem em conjunto pelos danos causados.

Violações de segurança podem resultar em multa de até 2% da receita anual da organização no Brasil e a multa máxima para cada violação é de 50 milhões de reais. A autoridade nacional competente definirá o nível de punição de acordo com a gravidade da falha. E antes que as sanções sejam impostas à organização, ela enviará alertas e orientações (arts. 52, 53 e 54 da LGPD).

Após a promulgação da LGPD, o Brasil entra para a lista dos 100 países mais adequados para proteger a privacidade e o uso de dados, sendo uma informação positiva, demonstrando a atuação do governo em relação à responsabilidade quanto à prevenção dos vazamentos de dados em massa, como as notícias constantemente noticiadas na mídia internacional (BIONI, 2019 *apud* AYRES, 2019).

Outro ponto importante é a adequação das empresas à lei, segundo Lívia Fiego para o Estadão:

> Uma pesquisa feita pela Akamai Technologies, empresa americana de serviços e performance de tráfego global na internet, realizada entre junho e julho deste ano com mais de 400 organizações que atuam no Brasil, apontou que 64% das empresas não estavam em conformidade com a LGPD ainda. O levantamento diz que 24% das empresas já estão se adaptando à legislação, outras 16% sabem da necessidade, mas ainda não iniciaram o processo e 24% ignoram do que trata a lei. (FIEGO, 2021)

Vislumbra-se que a adequação a legislação já está ocorrendo paulatinamente considerando todos os ajustes que as empresas terão de fazer em seus procedimentos e sistemas internos, assim, adaptando as exigências legais e promovendo uma maior segurança da informação e dos dados tratados.

CÁPITULO II - A VIOLAÇÃO DE DADOS NO BRASIL

2.1 A EXPOSIÇÃO NA INTERNET E COLETA DE DADOS

"*Data is the new oil*", em tradução livre "Dados são o novo petróleo", foi criada em 2006 por Clive Humby um matemático londrino especializado em ciência de dados.

Essa expressão tem sido bastante citada no mercado e executivos do mundo todo a usam para defender a ideia de que os dados são tão valiosos quanto o petróleo – o que aponta que, em tese, quem souber fazer bom uso deles e aproveitar todo seu potencial, só tem a ganhar.

Michael Palmer expandiu a determinada citação apontando que:

> Como o petróleo, os dados são valiosos, mas se não forem refinados, não podem realmente ser usados. (O petróleo) deve ser transformado em gás, plástico, produtos químicos etc., para criar uma entidade valiosa que impulsione atividades lucrativas; assim, os dados devem ser divididos e analisados para que tenham valor. (Tradução livre) (PALMER *apud* ARTHUR, 2013).

Para a Lei Geral de Proteção de Dados o conceito geral de dado pessoal é definido bastante abertamente como a "informação relacionada à pessoa natural identificada ou identificável" conforme seu art. 5º, ou seja, tudo aquilo que de alguma forma puder tornar identificável uma pessoa física será considerado um dado pessoal.

Portanto, se uma informação permite identificar, direta ou indiretamente, um indivíduo que esteja vivo, então ela é considerada um dado pessoal, como por exemplo: nome, RG, CPF, gênero, data e local de nascimento, telefone, endereço residencial, entre outros.

Dentro desse contexto, ainda há o conceito de dados pessoais sensíveis, que são aqueles que tem um grau ainda maior de tratamento para que eles possam ser utilizados. Dentro dos dados sensíveis, entram informações de orientação política, filosófica, questões de orientação sexual, dados de origem étnica, social, informações médicas, de saúde e biométricas.

Dada essa nova visão, tornou-se comum a coleta e utilização massiva de dados pessoais por organismos estatais e privados, em razão da expansão tecnológica e sua grande utilização, criando-se desafios ao direito à privacidade.

Em sua principal obra *Privacy in Context: Technology, Policy, and the Integrity of Social Life* [5](Inglês), Helen Nissenbaum, 2010, demonstra a necessidade de um contexto que enfatiza a maleabilidade da privacidade de acordo com o cenário, contextos nos quais cada vigilância, por exemplo as realizadas por câmera, podem ser pensadas como aceitáveis, ou o contrário.

Neste viés, o compartilhamento de dados de uma compra sem o consentimento do titular estão fora dos limites[6], ao passo que a instalação de câmeras em sinais de trânsito muitas vezes são consideradas legítimas.

Em suma, o controle sobre os dados se torna relativo e, segundo Helen Nissenbaum, invariavelmente contextual:

> Temos um direito à privacidade, mas não se trata de um direito de controlar informações pessoais, ou de um direito de limitar o acesso a estas informações. Em vez disso, é o direito de viver em um mundo no qual nossas expectativas sobre o fluxo de informações pessoais são, na maioria das vezes, atendidas; expectativas que são moldadas não apenas pela força do hábito e pelas convenções, mas devido a uma confiança geral no apoio mútuo que esses fluxos concedem aos princípios-chave de organização da vida social, incluindo os princípios morais e políticos. Esse é o direito que chamei de integridade contextual, alcançada através do equilíbrio harmonioso de regras sociais, ou normas, com valores, fins e propósitos locais e gerais. Isso nunca é uma harmonia estática, no entanto, porque, com o tempo, as condições mudam e os contextos e normas evoluem junto com eles. (Tradução livre) (NISSENBAUM, 2010, p. 231).

Assim sendo, cabe aqui ressaltar que a exposição e coleta de dados na internet deve ser contextual, conforme a teoria da integridade contextual (*contextual integrity*) formulada por Helen Nissenbaum, visto que ao fazer uma compra *on-line* é sabido que a loja terá suas informações de pagamento, dados cadastrais e endereço, no entanto ao utilizar um serviço de mensagens (WhatsApp LLC) não deveria se considerar legítimo a coleta de dados como nome, imagens e descrições de grupos que se faz parte, bem como nível da bateria e informações relacionadas a operadora que se utiliza (WHATSAPP, 2021). O que se agrava ainda mais ao serem compartilhados coercitivamente com outros serviços da empresa proprietária (Facebook), da qual o usuário pode ter nenhum vínculo anterior (SOUTO; MACHADO, 2021).

---

[5]Privacidade em contexto: tecnologia, política e integridade da vida social.
[6]TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO, COMARCA DE SÃO PAULO, FORO CENTRAL CÍVEL, 13ª VARA CÍVEL: 1080233-94.2019.8.26.0100.

Essa nova política de privacidade do WhatsApp (prevista para 15 de maio de 2021) já foi questionada no Ministério da Justiça e na ANPD pelo Idec (Instituto de Defesa do Consumidor) que enviou um documento a essas autoridades pedindo a suspensão da mudança dos termos de uso do aplicativo (SOPRANA, 2021).

A advogada Juliana Oms, uma das autoras do documento assevera que:

> Não está clara a base que explica o compartilhamento de dados entre as empresas. É para melhorar algoritmo do Instagram? É para fins de segurança do usuário? Eles citam que coletam dados como IP, de conexão, mas não são tão explícitos sobre quais dados compartilham entre as empresas. (SOPRANA, 2021)

Na opinião do Idec, o novo modelo do WhatsApp é um “consentimento forçado”, no estilo “aceite tudo ou vá embora”, o que se torna agressivo diante da adesão de brasileiros à plataforma, incorporada à rotina de trabalho e de comunicações de mais de 120 milhões de brasileiros (SOPRANA, 2021).

Os dados pessoais que são recolhidos num contexto e depois usados noutro contexto sem a consciência e consentimento do indivíduo acarreta graves violações individuais da privacidade (por exemplo, os dados pessoais que são partilhados por um utilizador para preencher uma transação comercial, mas são vendidos a um anunciante sem o conhecimento do indivíduo).

A transferência de dados entre os diversos contextos é um problema, especialmente, quando os utilizadores não têm conhecimento que isto está a acontecer.

No Brasil, antes do vigor da Lei Geral de Proteção de Dados, a coleta de dados ocorria de forma demasiada na qual boa parte dos dados sensíveis dos brasileiros eram comercializados em sites como “lembrete digital”, sendo esse responsável pela primeira ação civil pública com pedido de tutela oferecida pelo MPDFT, baseada na Lei Geral de Proteção de Dados Pessoais, no entanto, o juízo da 5ª vara Cível de Brasília indeferiu a inicial do MP/DF contra empresa que estaria comercializando dados pessoais pela internet após o site entrar “em manutenção” com o entendimento do julgador de que “os responsáveis pelo sobredito sítio devem estar buscando adequar os seus serviços às normas jurídicas de proteção de dados pessoais.”.

Uma vez que os utilizadores frequentemente têm pouco controle sobre o uso subsequente de dados que divulgam, muita da responsabilidade pelo uso apropriado de dados recai sobre o responsável pelo tratamento de dados.

Esta noção de integridade contextual implica um dever do responsável pelo tratamento de estar ciente do contexto em que os dados são recolhidos e a respeitar a integridade daquele contexto. Isto está relacionado com o princípio da “finalidade” no tratamento de dados de acordo com a LGPD, em razão de apenas coletar dados pessoais para fins legítimos, informando com clareza ao usuário a finalidade dessa coleta.

Contudo, ao navegar na web ou mesmo utilizar os aplicativos de e-mail e redes sociais diariamente se está vulnerável à métodos que expõem os nossos dados pessoais, sendo assim coletados por criminosos.

De acordo com um relatório da Norton Cyber Security, em 2017 o Brasil passou a ser o segundo país com maior número de casos de crimes cibernéticos, afetando cerca de 62 milhões de pessoas (UOL, 2018). Não obstante, com o acometimento da pandemia ataques direcionados a ferramentas que permitem acesso remoto ao trabalho aumentaram 333% no Brasil, entre fevereiro e abril de 2020, segundo levantamento da Kaspersky (OLIVEIRA; ROSSI, 2020).

Os cibercriminosos podem explorar pessoas e roubar suas informações confidenciais por meio de várias estratégias dentre elas o *Phishing*, que é um e-mail enviado por um criminoso da Internet disfarçado como um e-mail de uma fonte legítima e confiável; a mensagem tem o objetivo de induzi-lo a revelar informações relacionadas ou confidenciais.

Outra maneira sofisticada é o *Spoofing* que descreve um criminoso que se faz passar por outro indivíduo ou organização, com a intenção de recolher informações pessoais ou comerciais; este muito utilizado no Brasil como método de engenharia social em golpes de roubo de WhatsApp.

Além da técnica do *Pharming*, que consiste em um site malicioso que se assemelha a um site legítimo, usado para coletar nomes de usuários e senhas, golpe que cresceu bastante em razão do benefício do auxílio emergencial.

Outrossim, há empresas bilionárias (Facebook e Google) de olho nos dados pessoais, como consumo, gostos, movimentações, lugares frequentados entre outros,

das quais visam criar um perfil de cada usuário com o intuito de oferecer propagandas cada vez mais customizadas para o perfil (*profiling*[7]).

Essa estratégia de marketing direcionado tem um tipo de pensamento apoiado na compra de mídia que se baseia em duas premissas. A primeira é a do funil de conversão: a exibição da propaganda para mais pessoas pelo menor custo possível (na boca, parte superior do funil), torcendo pela conversão na parte de baixo. A segunda é a da segmentação da audiência: filtros para melhor escolher para quem a empresa quer mostrar os banners (público-alvo), cujos critérios costumam ser demográficos (idade, gênero, cidade, classe social etc.) ou muitas vezes baseados em inferências (pessoas que já navegaram no site, entraram na loja, cadastros no banco de dados etc.) (TEIXEIRA, 2020).

Neste grande exercício de “cercar o cliente”, profissionais de marketing vão empurrando milhares de consumidores de um campo aberto para um caminho estreito, baseado em um pensamento que é classificado como “de fora para dentro”.

Essa estratégia só é possível com a utilização de pequenos arquivos de dados colocados em seu computador ou dispositivo móvel quando se visita um site, chamados de *cookies*.

Os *cookies* são amplamente utilizados por fornecedores de serviços *on-line* para (por exemplo) fazer com que os seus sites ou serviços funcionem, ou para funcionar de forma mais eficiente, tal qual para fornecer informações de relatórios (Tradução livre) (INDIANA UNIVERSITY, 2018).

Esses pequenos arquivos geralmente contêm informações sobre visitas ao sítio, assim como quaisquer informações/dados que tenham sido fornecidas pelo indivíduo como voluntário, ou seja, ao aceitar as preferências de cookies em um site que adere a essa opção, o servidor coloca as informações nele, desta forma, quando se retorna ao site, ele usa as informações do cookie para criar uma página personalizada para o internauta.

Desta forma, são comumente usados para rastrear a atividade na web, funcionando como um cartão de identificação. Logo, um servidor da internet pode

---

[7] O *profiling*, segundo Danilo Doneda, consiste na elaboração de perfis de comportamento de uma pessoa (ou de um grupo de pessoas) a partir de suas informações pessoais, que podem ser disponibilizadas por ela mesma ou que são colhidas. (DONEDA, 2006. p. 173 *apud* DE LIMA, 2019, p. 34)

coletar informações sobre quais páginas da rede são mais usadas e quais páginas estão obtendo mais acessos repetidos para assim fornecer páginas com conteúdo personalizado.

As lojas *on-line* costumam usar *cookies* que registram qualquer informação pessoal inserida, como também quaisquer itens no carrinho de compras eletrônico, de forma que não seja necessário inserir essas informações novamente cada vez que visitar o site. Outro exemplo bastante comum são as compras *on-line* de passagens aéreas das quais podem variar de valor em razão da coleta das informações dos *cookies* do dispositivo (WEISS *apud* MCGEE, 2013).

No entanto, frequentemente há fortes incentivos para os responsáveis pelo tratamento de dados pessoais (Controlador ou Operador) os transferirem de um contexto para outro, por exemplo, retirar os dados das transações dos clientes e vendê-los para que possam ser usados para publicidade direcionada.

Essa estratégia de direcionamento (*targeting*) leva a uma relação agressiva, irracional da sociedade capitalista e a busca do indivíduo para realizar-se, desta maneira, direciona às práticas que exaltam o prazeroso, o opulente e o supérfluo.

Com a sua abundância de produtos, serviços, a sociedade de consumo manifesta a magnitude da técnica de sedução. Bauman confirma isto, quando externa que “(...) quanto maior a demanda de consumo (ou seja, quanto mais eficaz for a sedução de potenciais clientes), mais segura e próspera será a sociedade de consumo (...)” (BAUMAN, 2008, p. 164 *apud* LAGO; REIS, 2016, p. 46).

O comportamento do consumidor é guiado por uma atitude quase irracional causado pelos poderosos métodos de publicidade das empresas. Cientistas nas áreas de publicidade, marketing, entre outros, estudam o comportamento do consumidor por muitos anos e as maneiras de induzi-los a consumir. Nos shoppings, galerias, lojas, é realizado o processo de climatização, e é criada uma atmosfera de “eterna primavera” para celebrar o consumo: “Vivemos desta maneira ao abrigo dos signos e na recusa do real. (...) A imagem, o signo, a mensagem, tudo o que ‘consumimos’, é a própria tranquilidade selada pela distância ao mundo e que ilude, mais do que compromete, a alusão violenta ao real” (BAUDRILLARD, 2007, p. 25, *apud* NETO, 2009, p. 175).

O comportamento impulsivo atinge a todos os cidadãos, mesmo os consumidores com alto nível de escolaridade, supostamente não tão suscetíveis a

serem tapeados, mas caem nas armadilhas do *marketing*[8] que gera demandas e manipula as formas como demonstram seu poder, levando-os a crer que serão admirados e considerados bem-sucedidos, bonitos ou felizes se obtiverem determinado produto.

Um exemplo dessa publicidade está nos aplicativos de buscas ou nas redes sociais que se visita, tanto Google quanto Facebook utilizam-se de anúncios personalizados a partir de uma modelagem dos dados obtidos de seus usuários. A veiculação desses anúncios são cada vez mais específicas e chegam a ser preditivas, quase como um guia do que fazer, comprar e consumir.

Essa técnica chamada *marketing* preditivo segundo a Salesforce é o *marketing* que usa *big data*[9] para desenvolver previsões precisas do comportamento futuro do cliente. Mais especificamente, o *marketing* preditivo usa ciência de dados para prever com precisão quais ações e estratégias que têm maior probabilidade de sucesso.

Em suma, a inteligência preditiva orienta as decisões de publicidade e propaganda a fim de gerar/impulsionar um desejo latente de consumo para os utilizadores de seus serviços.

Esse desejo de transcender suas possibilidades econômicas para obter tudo o que os meios de comunicação consideram indispensável tem como consequência o superendividamento. Sem mencionar os casos de consumo compulsivo, ainda mais graves, dada a vulnerabilidade desse tipo de consumidor – tido até mesmo como doente, vez que é comparado a vítimas de patologias como cleptomania, bulimia, ludopatia, entre outras (TOLEDANO BARRERO, 1998, p. 493, *apud* NETO, 2009, p. 176). Esta doença também tem nome: oniomania ou oneomania, do grego *onios* (compra). Para estes consumidores, o ato de comprar relaciona-se unicamente ao suprimento de um desejo incontrolável, não pelo produto, mas pelo ato de consumir, e não consideram o desfrute ou utilidade do bem adquirido (BERTONCELLO, 2006, p. 59, *apud* NETO, 2009, p. 176).

---

[8] Atividade com o intuito de compreender as necessidades dos clientes para assim elaborar estratégias de comunicação e venda de produtos e serviços.

[9] É a área do conhecimento que estuda como tratar, analisar e obter informações a partir de conjuntos de dados grandes demais para serem analisados por sistemas tradicionais.

Essas consequências devastadoras (em alguns casos) podem ser suprimidas quando se respeita as necessidades do consumidor e sua privacidade, segundo Rodrigo Ghedin, criador do blog Manual do Usuário:

> O intuito de toda essa vigilância é reduzir você, pessoa física dotada de livre arbítrio, a uma fórmula algorítmica capaz de revelar suas fraquezas cognitivas e explorá-las para induzi-lo a consumir mais notícias, mais vídeos, mais assinaturas, mais serviços e produtos, mais, mais e mais. (...) Uns podem dizer que se trata de um efeito colateral da inevitável transformação da internet em um grande balcão de negócios. Pode ser. O problema é que essa dinâmica virou regra e engoliu até mesmo iniciativas simples, sem qualquer grande pretensão comercial. (GHEDIN, 2019).

Portanto, as políticas da proteção de dados têm de assegurar que esta descontextualização não deverá ser feita em detrimento do titular de dados, também assegurar que o titular de dados tem oportunidade de expressar e aplicar as preferências sobre se, quando ou como isto deve acontecer e garantir a anonimização dos dados[10].

A Lei Geral de Proteção de Dados (LGPD) atua na intermediação, na comunicação entre os usuários e as empresas passando a mensagem de que elas devem se adequar às normas de coleta e utilização de dados pessoais, não sendo mais viável que escolham de que forma vão agir, em síntese, o usuário passa a opinar e reivindicar os direitos que têm.

2.2 FALTA DE SEGURANÇA DA INFORMAÇÃO E COMPARTILHAMENTO IRREGULAR DE DADOS

A sociedade brasileira vive uma crescente digitalização sendo uns dos países mais conectados do mundo, com 150,4 milhões de internautas - 71% da população -, conforme o relatório We Are Social da Hootsuite que também mostra que 66% da população brasileira são usuárias ativas de redes sociais (KEMP, 2020).

Tendo em vista essa crescente exposição da sociedade brasileira que a tecnologia da informação gera, frequentemente acontecem diversos casos de violação de dados pessoais e de vazamentos de informações, expondo dados e informações confidenciais dos titulares.

---

[10] (...) um processo pelo qual é quebrado o vínculo entre o(s) dado(s) e seu(s) respectivo(s) titular(es), o que é chamado de anonimização. Esse processo pode se valer de diferentes técnicas que buscam eliminar tais elementos identificadores de uma base de dados, variando entre: a) supressão; b) generalização; c) randomização e; d) pseudoanonimização.

Cabe salientar que um vazamento é definido como um evento em que a identificação de uma pessoa a um registro médico e/ou um registro financeiro ou cartão de débito estão potencialmente ou já em risco, seja em formato eletrônico ou em papel.

A cientista da computação Nina da Hora em seu artigo para a revista Technology Review, do MIT, assevera que:

> Nossos dados pessoais fazem parte de um aglomerado de informações sujeitas a exposições. Isso ocorre porque a nossa segurança depende de terceiros, meros desconhecidos que detêm o controle cibernético. Um exemplo disso é o momento em que aceitamos os termos de privacidade sem uma avaliação cuidadosa. (DA HORA, 2021).

Em razão desse controle cibernético há diversos personagens que detém essas informações pessoais, sendo suas capacidades de processamento de obtê-los e de resguardá-los com segurança o que os diferencia, visto que são necessários requisitos mínimos para isso.

De acordo com um estudo do Instituto Pomenom sobre o custo de uma violação de dados, o Brasil é o país com a maior propensão ao vazamento de dados, com uma probabilidade de 43% envolvendo um mínimo de 10.000 registros para amostra do país durante um período de 24 meses conforme pesquisa de 2018.

Ademais, conforme o Relatório Anual 2020 de Atividade Criminosa On-line no Brasil, elaborado pela empresa de cibersegurança Axur, em 2020, o país foi campeão em vazamentos de dados de cartões, acumulando sozinho 45,4% do total de casos registrados no mundo, distante do segundo colocado, os EUA (34,3%) (CARDOSO, 2021).

Como já dizia Antônio Carlos Jobim “O Brasil não é para principiantes” (DE MORAES, 2014), a marola de vazamentos de dados tem se tornado um tsunami, ainda mais com o recente mega vazamento de dados de 223 milhões de brasileiros (G1, 2021), o que põem em risco a segurança digital de uma nação e faz nos questionar “os nossos dados pessoais estão seguros diante da LGPD e suas sanções?”.

A falta de segurança da informação é generalizada e o compartilhamento irregular é feito com olhos fechados por aqueles que detém significativos bancos de dados pessoais.

Para a cientista da computação Nina da Hora:

> (...) quando falamos de Segurança da Informação não estamos apenas falando sobre proteção de senhas. Estamos debatendo sobre a entrada e o armazenamento das nossas informações pessoais em todos os âmbitos e por empresas e terceiros que não conhecemos. Pensar em uma sociedade digital inclui pensar na união das vulnerabilidades preexistentes em um mundo sem internet e que agora intensificam-se e agravam-se quando não são postas de maneira clara e acessível aos usuários. (DA HORA, 2021).

No relatório sobre o prejuízo de um vazamento de dados 2020 conduzido pela IBM Security as causas principais de um vazamento de dados foram agrupadas em três categorias: falhas no sistema, incluindo falhas de processos de TI e de negócios; erro humano, incluindo funcionários negligentes ou contratados que, sem querer, causaram um vazamento de dados; e ataques mal-intencionados, que podem ser causados por hackers ou criminosos. Sendo que 52% da parcela total de vazamentos são causados por ataques mal-intencionados, empregando um prejuízo médio de US$ 4,27 milhões.

Desta maneira, são necessários requisitos mínimos de segurança da informação e políticas que visam uma forma segura de tratamento de dados. De acordo com o Guia de Boas Práticas da LGPD apresentados pelo Governo Federal, dentre elas a Privacidade desde a concepção e por padrão (Privacy by Design e by Default), a implantação de Padrões, Frameworks e Controles de Segurança da Informação como sistemas de gestão de riscos e técnicas de segurança. Também vale ressaltar a adoção de *firewalls*[11], IPS (Sistema de Prevenção de Intrusos, do inglês Intrusion Prevent System), roteadores, anti-DDOS[12], monitoramento constante de rede, correlacionador de eventos, profissionais treinados em monitoração e em forense computacional bem como seguir princípios de governança e controle, que significa garantir transparência, auditabilidade, comunicação adequada e integração entre os níveis decisório e executório da proteção à informação.

No entanto não só de vazamento ou exposição de dados estamos vulneráveis, há incontáveis empresas que compartilham irregularmente dados pessoais antes mesmo do início da vigência da LGPD, da qual refletiam justamente o que seria

[11] Uma solução de segurança baseada em hardware ou software (mais comum) que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas.

[12] Evitar com que aconteça uma sobrecarga em um servidor ou computador comum para que recursos do sistema fiquem indisponíveis para seus utilizadores.

acompanhado com atenção redobrada pela SENACON: captura de informações, sem consentimento, para fins comerciais.

Em razão da intensificação do acompanhamento de práticas que possam constituir os chamados “ilícitos de consumo” no ambiente digital, a SENACON após uma semana da vigência da LGPD já contava com 34 processos administrativos em andamento envolvendo o uso indevido de dados pessoais de usuários de plataformas digitais, destes, boa parte dos processos envolve as principais gigantes americanas de tecnologia (CAMAROTTO, 2020).

À frente da SENACON desde agosto, Juliana Domingues diretora do Departamento de Defesa do Consumidor, em entrevista para o Valor Econômico lembra que processos como esse visam averiguar se a política de privacidade das plataformas foi devidamente desenhada para deixar clara anuência quanto ao compartilhamento dos dados (CAMAROTTO, 2020).

Dentre esses processos, Murillo Camarotto, pesquisador no Reuters e jornalista no Valor Econômico destaca:

> A plataforma de relacionamentos Tinder, por exemplo, é investigada por suposto compartilhamento, com várias empresas, de dados de localização, endereço IP, idade e sexo dos usuários. O objetivo seria o aprimoramento de anúncios publicitários para esse público. (CAMAROTTO, 2020).

Outro caso parecido foi o do Facebook, que foi multado em R$ 6,6 milhões por ter adotado de forma considerada abusiva uma prática conhecida como “opt-out”, que é quando o usuário fornece dados para concluir certa tarefa (como uma compra), mas as informações são usadas para outros fins. A SENACON entendeu que a plataforma não tomou medidas para “evitar exposição desses dados a desenvolvedores nocivos”.

O compartilhamento irregular ainda é uma realidade explicitamente escancarada, da mesma forma um caso a se observar é da Serasa Experian que segundo a investigação da Unidade Especial de Proteção de Dados e Inteligência Artificial (Espec) do MPDFT identificou a venda de uma série de informações dos consumidores. Entre elas, estão nome, CPF, endereço, números de telefones, localização, perfil financeiro, poder aquisitivo e classe social, com a estimativa de que a Serasa tenha colocado à venda dados de mais de 150 milhões de brasileiros (MPDFT, 2020).

Ao comercializar dados pessoais dos cadastrados, a Serasa S.A. ultrapassa o limite permitido pela legislação brasileira e fere o direito à privacidade das pessoas, bem como seus direitos à intimidade e à imagem, o que inclui o direito à proteção de seus dados pessoais.

Cabe notar que os dados desse birô de crédito já estavam catalogados sem uma expressa ressalva dos seus respectivos titulares, assim sendo, o órgão alegou que a prática representa uma violação da Lei Geral de Proteção de Dados (LGPD), que oferece para o titular dos dados poder sobre como eles serão utilizados, afirmando:

> (...) para que o tratamento de dados seja fundamentado no legítimo interesse do controlador é necessário que seus propósitos sejam legítimos, específicos, explícitos e informados ao titular do dado, sendo que as finalidades do tratamento devem ser compatíveis com aquelas informadas ao titular, bem como que o tratamento seja limitado ao mínimo necessário à realização de suas finalidades, trazendo clara obediência aos princípios da finalidade, da adequação e da necessidade preconizados na Lei Geral de Proteção de Dados (artigo 6º, incisos I, II e III, da Lei n. 13.709/2018). (MPDFT, 2020).

Levando em consideração os casos apresentados de compartilhamento irregular de dados, urge necessário demonstrar as medidas tomadas em casos em que se deu um desfecho conforme o ordenamento pátrio e a LGPD, que é o instrumento legal para proteger, preservar e evitar irregularidades dos dados colhidos dos usuários, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Uma vez que as empresas cometerem vazamentos de dados ou os compartilharem irregularmente, ainda que de forma acidental, estarão sujeitas a diversas penalidades.

Para tanto, é fundamental que as organizações mapeiem os dados pessoais; identifiquem o percurso (portas de entrada e de saída), os locais em que estão armazenados, analisem se existem dados pessoais sensíveis e implementem mecanismos de segurança da informação e de proteção de dados pessoais.

Ademais, caso não seja possível a adoção desse fluxo, ou mesmo que adotado provoque falhas que gerem riscos aos dados coletados, a solução a ser adotada neste caso, será a imposição de sanções dispostas pelas normas vigentes com intuito de resguardar o direito e punir os violadores.

CÁPITULO III - LGPD DAS SANÇÕES E ANÁLISE DE CASOS

3.1 SANÇÕES DA LGPD, CASOS ANTERIORES À SUA VIGÊNCIA COM UMA ANÁLISE SEGUNDO A TEORIA DA INTEGRIDADE CONTEXTUAL

Na última década, uma grande e opaca indústria acumulou uma quantidade cada vez maior de dados pessoais. Um complexo ecossistema de sites, aplicativos, empresas de mídia social, corretores de dados e empresas de tecnologia de publicidade passaram a rastrear usuários *on-line* e *off-line*, coletando seus dados pessoais. Esses dados são reunidos, compartilhados, agregados e monetizados, alimentando uma indústria de 227 bilhões de dólares por ano (GRÖNE; PÉLADEAU; SAMAD, 2019). Isso ocorre todos os dias, conforme as pessoas vivem diariamente suas vidas, muitas vezes sem seu conhecimento ou permissão.

As facetas dessas empresas muitas das vezes não são conhecidas do grande público, vindo à tona a partir de escândalos ou vazamentos. Em 2018, por exemplo, não era notório o conhecimento da Cambridge Analytica antes do escândalo da coleta de informações pessoalmente identificáveis de até 87 milhões de usuários do Facebook (SOLON, 2018).

Em razão disso, torna-se indispensável uma regulação para o tratamento de dados e sanções para estas condutas que lesam de maneira significativa os seus titulares.

No Brasil, a Lei Geral de Proteção de Dados (LGPD) é o marco regulatório do tratamento de dados pessoais (art. 1º)[13] e apresenta um rol de sanções em seu art. 52[14], aplicáveis aos agentes de tratamento de dados em razão de infrações cometidas às normas previstas na lei, assim, visa prevenir os dados pessoais diante dos potenciais violadores.

O art. 52 da lei 13.709/18 apresenta um rol destas sanções que serão aplicadas pela Autoridade Nacional em hipótese de infração às normas previstas nesta lei. É interessante compreender que as sanções se aplicam à infração de qualquer norma

---

[13] Art. 1º - Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

[14] 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

prevista na LGPD. Isso quer dizer que se atentar aos princípios é tão relevante quanto observar dispositivos de caráter mais pragmático/objetivo.

Dentre estas sanções, a primeira penalidade estipulada pela lei é a advertência, considerada o tipo mais leve dentre as sanções administrativas. Embora pareça inofensiva, é importante enfatizar que a advertência indicará um prazo para adoção de medidas corretivas. Caso ocorra inércia da advertida e a não adoção de medidas dentro do prazo especificado pode constituir uma nova infração e resultar em sanções mais severas para a empresa.

A segunda sanção a que se refere a lei são as multas simples. O valor da multa pode chegar em até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, no entanto, é limitada ao total de R$ 50 milhões por infração.

Devemos nos atentar ao “por infração”: ainda existe incerteza se a Autoridade Nacional de Proteção de Dados (ANPD) irá considerar como uma única infração, mas podemos pensar em infração como cada incidente ou cada dispositivo violado da lei em um único incidente (há ainda aqueles que arriscam mais alto e entendem que poderia ser, inclusive, o valor pago por cada dado vazado, por exemplo, embora pareça improvável, não é impossível).

Além da multa simples, o art. 52 traz uma outra modalidade de multa: as multas diárias, observando o mesmo limite imposto na multa simples. Considerando que, ainda com esse limite máximo, a possibilidade de emprego de multas diárias podem causar prejuízos consideráveis ao infrator, podendo de fato, atingir de forma significante o faturamento de empresas que talvez R$ 50 milhões, por si só, não represente um impacto econômico significativo.

Embora as multas se destaquem entre as infrações, é importante considerar que os danos indiretos podem ser maiores que os diretos: perda de valor da marca, impacto na confiança do cliente e do investidor, desvalorização de ativos e perdas de contratos são apenas alguns deles. Em razão isso, dependendo da natureza da infração e do ramo de negócios, a publicização talvez traga maior impacto que a multa. Ela está entre as sanções dispostas no art. 52, e só pode ser aplicada após a devida apuração do caso e confirmação da ocorrência.

Por fim, temos duas outras formas de sanções que também afetam indiretamente o negócio e podem significar uma paralisação parcial das operações e

perda de ativos: o bloqueio e a eliminação dos dados pessoais referentes à infração. No primeiro caso até a sua devida regularização.

Todas as sanções mencionadas somente serão aplicadas após procedimento administrativo que assegure a ampla defesa do acusado. Desta forma, serão consideradas as particularidades de cada caso em específico, assim, a lei traz alguns parâmetros e critérios para a avaliação daquilo que será aplicado no caso concreto, tais como: A gravidade e a natureza das infrações e dos direitos pessoais afetados, boa-fé, reincidência, o grau do dano, cooperação do infrator, condição econômica, vantagem auferida ou pretendida pelo infrator, adoção de política de boas práticas e governança, adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, adoção de medidas corretivas e a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Apesar da coerência das sanções e sua aplicabilidade, ante a inerente problemática normativa brasileira, existe um risco regulatório sancionador dado o desacordo entre a entrada em vigor da LGPD e dos artigos que regulam as sanções pelas infrações eventualmente cometidas.

Há de se aguardar até 1º de agosto de 2021 para que as infrações sejam devidamente aplicadas ou pior, as infrações praticadas não serem averiguadas em razão de conciliação direta do controlador com o titular ou prescrição da infração/multa[15], a ser definida pela ANPD. Considerando a ausência da Autoridade Nacional de Proteção de Dados (ANPD), não há previsão de instauração de procedimentos administrativos com fundamento na norma de proteção de dados, visto que a aplicação das sanções previstas na lei compete exclusivamente à ANPD.

No entanto, atualmente o Marco Civil da Internet apresenta diversas penalidades que podem ser aplicadas ou mesmo a aplicação do Código de Defesa do Consumidor tendo em vista haver geralmente uma relação de consumo anterior com a suposta empresa infratora na coleta de dados.

Cabe destacar que o compêndio consumerista já foi fundamento para a aplicação de indenizações aos vazamentos e compartilhamentos irregulares

[15] Agência Espanhola de Proteção de Dados prevê apenas multas administrativas. Da qual o prazo de prescrição para infrações de proteção de dados vai de 1 a 3 anos, dependendo da infração e gravidade, tal como o prazo de prescrição para multas da mesma maneira ocorre entre 1 e 3 anos. (ESPAÑA. Ley Orgánica 3/2018)

anteriores a vigência da Lei Geral de Proteção de Dados, uma vez que ela não substitui as aplicações de sanções administrativas, civis ou penais definidas na Lei nº 8.078/1990 e em legislação específica.

Conforme preceitua Bruno Bioni (2020, p. 258-259):

> Diferentemente dos métodos tradicionais de hermenêutica, que rogam pela prevalência de uma norma sobre a outra, a teoria do diálogo das fontes propõe uma nova teoria geral do direito visando à intersecção e complementação das normas. Em vez de uma monossolução, passa-se a adotar uma lógica de coordenação pela qual deve haver aproximação e não afastamento em um ambiente normativo plúrimo. Pavimenta-se, com isso, uma via para que haja influência recíproca entre as normas, isto é, um verdadeiro diálogo. A esse respeito, é importante destacar que a própria LGPD acenou para tal intersecção ao pontuar que não estão excluídos outros direitos e princípios relacionados à matéria previstos no ordenamento jurídico brasileiro.

Dessarte, cabe analisar as sanções aplicadas aos vazamentos e compartilhamentos irregulares de dados à luz dos pressupostos normativos aqui expostos, o que conduz a uma interpretação mais abrangente, ou seja, anterior a vigência da LGPD que é de fundamental importância para a sua atual aplicabilidade, e com sua corrente vigência, porém com a ressalva de uma ANPD em construção, acarretando o seu emprego por outros órgãos e poderes.

Desta forma, antes da vigência da lei em 2020, no final de 2017 e início de 2018, há um caso interessante da loja de artigos esportivos Netshoes da qual foram vazadas duas listas de credenciais com informações sobre 1.999.704 clientes. Entre os dados expostos, estavam nome completo, e-mail, CPF, data de nascimento e produtos comprados.

Segundo o Ministério Público do Distrito Federal e Territórios (MPDFT) à época, este foi “um dos maiores incidentes de segurança registrados no Brasil” (VENTURA, 2019). Inicialmente, a empresa entrou em contato com alguns clientes, no entanto, apenas através de um e-mail genérico sobre segurança. Após recomendação do *parquet*, a empresa comunicou que iria ligar para os quase 2 milhões de consumidores afetados.

A Netshoes colaborou em diversos aspectos durante a investigação do caso, inclusive fornecendo dados pessoais comprometidos aos quais o MP não tinha acesso. Por isso, as duas partes chegaram em 2019 a um acordo na forma de um TAC (Termo de Ajustamento de Conduta).

A empresa se comprometeu a pagar indenização de R$ 500.000,00, que seriam recolhidos mediante depósitos no Fundo de Defesa de Direitos Difusos (FDD), além do cumprimento de outras obrigações, caso ocorresse inércia da compromissária, cabível ação de reparação pelos danos morais coletivos causados.

Para o promotor de Justiça Frederico Meinberg Ceroy, compromitente do referido TAC:

> A assinatura do presente Termo de Ajustamento de Conduta demonstra ser possível a resolução de conflito de forma consensual, com o devido ressarcimento da coletividade ante ao dano moral sofrido, sem, contudo, onerar excessivamente a empresa que colaborou com as investigações do MP. (MPDFT, 2019).

Neste TAC o MPDFT se embasou na legislação aquela época vigente especialmente na adoção de uma fundamentação suplementada no Marco Civil da Internet considerando que ele assegura, aos titulares dos dados pessoais, os direitos de inviolabilidade da intimidade e da vida privada, bem como o direito de não fornecimento a terceiros dos dados pessoais, salvo mediante consentimento livre expresso e informado. E do Código de Defesa do Consumidor, haja vista a defesa dos interesses e direitos dos consumidores e das vítimas poderá ser exercida em juízo individualmente ou a título coletivo, considerando que a efetiva prevenção e reparação de danos são direitos básicos dos consumidores.

Cabe ressaltar, que foi utilizada a título de orientação a Lei n. 13.709/18 (LGPD) que ainda não vigorava, para orientar a adoção de 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.

Outro caso de vazamento de dados relativamente grave e digno de explanação é do Banco Inter, cujo, em julho de 2018 uma investigação do MPDFT revelou que havia vazado dados pessoais de 19.961 correntistas.

A Unidade Especial de Proteção de Dados e Inteligência Artificial (Espec) do MPDFT ajuizou uma Ação Civil Pública por Danos Morais Coletivos (ACP) no valor de R$ 10 milhões, a título de indenização, em razão de não ter tomado os cuidados necessários para garantir a segurança dos dados pessoais de seus clientes e não clientes.

À época o Banco tentou encobrir o vazamento alegando que as notícias visavam “prejudicar a reputação do Banco Inter. Considerando que não houve invasão e, tampouco comprometimento dos sistemas de segurança do banco” (ISTOÉ, 2018). Ressaltou o signatário da ACP o promotor de Justiça Frederico Meinberg:

> As tentativas de encobrir o incidente de segurança, promovidas pelo Banco Inter, geraram prejuízos morais e insegurança aos clientes, não clientes, investidores, acionistas, ecossistemas de Fintechs e Startups brasileiros de dados, bem como na confiabilidade da migração dos serviços de processamento, armazenamento e de computação em nuvem das instituições financeiras. (MPDFT, 2018).

A Ação Civil Pública ajuizada se norteou pelo Código de Defesa do Consumidor, uma vez que é possível veicular qualquer espécie de tutela jurisdicional para a defesa dos direitos e interesses protegidos pelo CDC[16], razão pela qual se pleiteou o pedido de natureza indenizatória por danos morais coletivos.

O dano moral vem expresso no artigo 6º, inciso VI, do CDC, que dispõe acerca dos direitos básicos dos consumidores, entre eles o da efetiva prevenção e reparação de danos patrimoniais e morais, individuais, coletivos e difusos.

Na medida em que inegavelmente, a demanda possuía essência e contornos coletivos, tendo em vista a quantidade de consumidores clientes e não clientes[17] (*Bystanders*) do Banco Inter afetados pelo incidente de segurança.

O *parquet* orientou-se pelo enunciado da Súmula 297 do Superior Tribunal de Justiça - STJ[18], ou seja, os contratos firmados entre cliente e banco devem obedecer ao Código de Defesa do Consumidor, isto porque, o pacto firmado entre as partes constitui nitidamente uma relação de consumo. Assim, arguiu que os bancos respondem objetivamente pelos danos causados aos seus clientes, como dispõe o artigo 14, § 1º, do Código de Defesa do Consumidor[19].

---

[16] Art. 83. Para a defesa dos direitos e interesses protegidos por este código são admissíveis todas as espécies de ações capazes de propiciar sua adequada e efetiva tutela.
[17] Art. 17. Para os efeitos desta Seção, equiparam-se aos consumidores todas as vítimas do evento.
[18] Súmula 297 - O Código de Defesa do Consumidor é aplicável às instituições financeiras.
[19] Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos. § 1° O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais: I - o modo de seu fornecimento; II - o resultado e os riscos que razoavelmente dele se esperam; III - a época em que foi fornecido.

Como é sabido, a atividade bancária deve garantir a segurança não só do patrimônio como também da integridade físico-psíquica do consumidor, haja vista os riscos inerentes deste tipo de atividade, referindo-se ao entendimento do Superior Tribunal de Justiça na Súmula 479[20], posto que a garantia da segurança ao patrimônio e à integridade físico-psíquica do consumidor é inerente à atividade bancária. Nesta perspectiva, nos casos de danos causados ao consumidor por ações ilícitas de terceiros, deve-se reconhecer a responsabilidade dos bancos, sob o fundamento de que tais fatos estão inseridos nos riscos desse tipo de atividade, tratando-se de fortuito interno.

No entanto, em 18 de dezembro o Banco celebrou com o MPDFT, no âmbito da ação civil pública de número 0721831-64.2018.8.07.0001, que tramitou perante a 15ª Vara Cível de Brasília, um acordo judicial, homologado pela mesma vara.

A instituição bancária acordou em pagar R$ 1,5 milhão como forma de reparar os danos morais coletivos de caráter nacional decorrentes do vazamento de dados de mais de 19 mil correntistas. Esse valor seria destinado a instituições públicas que combatem crimes cibernéticos, indicadas pelo MPDFT e instituições de caridade de forma conjunta.

O termo pactuado “Com esse acordo, permitiu-se uma resposta rápida à sociedade, bem como o aprimoramento do combate aos crimes cibernéticos no Brasil, em prol do interesse público e social, além do fomento do diálogo com o setor privado”, informou o coordenador da Espec, promotor de Justiça Frederico Meinberg (MPDFT, 2018).

Cabe aqui, demonstrar a contextualização desses dois casos conforme a teoria da integridade contextual de Helen Nissenbaum. O vazamento de dados da Netshoes atingiu cerca de 2 milhões de clientes da qual encerrou-se com um acordo de 500 mil reais. Enquanto o vazamento de dados do Banco Inter que atingiu cerca de 19 mil clientes, considerado “menor”, a partir de uma percepção quantitativa, encerrou-se com um acordo três vezes maior, ou seja, de 1,5 milhão de reais.

A verificação da violação da privacidade sob a perspectiva da teoria requer a análise de uma série de critérios, tais como contextos (ambientes sociais

[20] Súmula 479 - As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias.

estruturados), atores (emissores, receptores e sujeitos da informação), atributos (tipos de informação) e princípios de transmissão (confidencialidade, reciprocidade, necessidade etc.). Assim, nesses casos faz-se necessária uma avaliação mais ampla sobre os riscos causados pelo fluxo de informações à autonomia e à liberdade do indivíduo, assim como à igualdade, à justiça e à democracia.

Esta noção de integridade contextual implica um dever do responsável pelo tratamento de estar ciente do contexto em que os dados são recolhidos e a respeitar a integridade daquele contexto. Nestes casos, é notória a finalidade da coleta desses dados como também a privacidade e segurança para resguardá-los.

Entre os dados expostos pela Netshoes compreendiam nome completo, e-mail, CPF, data de nascimento e produtos comprados. Enquanto os dados de 13.207 correntistas que foram vazados pelo Inter, consistiam em informações bancárias, como número da conta, senha, endereço, CPF e telefone. Também foram comprometidos outros 4.840 dados de clientes de outros bancos que fizeram transações com os usuários do banco.

Isto posto, os dados bancários são muito mais significantes, refletindo em uma infração de alta gravidade, visto que se pode extrair os comportamentos bancários desses titulares afetados, ou seja, pagamentos, transferências, investimentos etc. Em contrapartida, o vazamento da Netshoes por mais que atingisse uma cifra maior de clientes, não refletiu numa gravidade elevada em razão de que não foram expostas informações relevantes como meio de pagamento e endereço.

Além do mais, Patrícia Peck Pinheiro em seu livro a Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018 (2018, p. 110) assenta que:

> Observando o princípio constitucional da proporcionalidade, a imputação das sanções deve sempre observar a proporcionalidade como um critério para prevenir e inibir possíveis abusos do poder estatal no momento do exercício de suas funções.

Esses casos apresentam a forma como se adequava a legislação brasileira antes da vigência da LGPD, da qual se procurava dar um desfecho satisfatório ante as normas vigentes à época.

3.2 CASO CYRELA E A CONCRETIZAÇÃO DO DIREITO À PRIVACIDADE PERANTE O STF.

Destarte cabe aqui apresentar casos com a lei em vigor, mas que infelizmente não foi possível aplicar as sanções do art. 52 em razão da disparidade já exposta.

Um desses casos é da construtora Cyrela, em que a justiça de São Paulo determinou o pagamento de uma indenização de R$ 10 mil por danos morais a um cliente, em uma das primeiras decisões judiciais por infração à Lei Geral de Proteção de Dados (LGPD), que entrou em vigor no dia 18 de agosto de 2020.

Em petição inicial, o titular dos dados informou que após a aquisição de um imóvel, recebeu contatos não autorizados de instituições financeiras, consórcios, empresas de arquitetura e de construção e fornecimento de mobiliário planejado.

Na decisão proferida pela juíza Tonia Yuka Koroku, da 13ª Vara Cível do Foro Central de São Paulo, relata que:

> (...) “parceiros” obtiveram os dados do autor para que pudessem fornecer a ele serviços estranhos aos prestados pela própria requerida. No entanto, cientes especificamente do empreendimento em relação ao qual o autor adquiriu uma unidade autônoma. Inclusive com propostas para pagamento do preço do imóvel por financiamento ou consórcio e compra e instalação de móveis planejados para o bem. (TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO. SENTENÇA: 1080233-94.2019.8.26.0100).

A magistrada assevera que os dados independentemente de sensíveis ou pessoais (art. 5º, I e II, LGPD)[21] foram tratados em violação aos fundamentos de sua proteção (art. 2º, LGPD)[22] e à finalidade específica, explícita e informada ao seu titular (art. 6º, I, LGPD)[23].

O contrato firmado entre as partes prescreveu apenas a possibilidade de inclusão de dados do requerente para fins de inserção em banco de dados (“Cadastro Positivo”), sem que tenha sido efetivamente informado acerca da utilização dos dados para outros fins que não os relativos à relação jurídica firmada entre as partes. Entretanto, houve a utilização para finalidade diversa e sem que o autor tivesse

---

[21] Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

[22] Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: (...)

[23] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

informação adequada (art. 6º, II, LGPD)[24]. Nesse mesmo sentido, defende o disposto no artigo 6º, III e IV, do Código de Defesa do Consumidor:

> Art. 6º São direitos básicos do consumidor:
> III - a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem;
> IV - a proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais, bem como contra práticas e cláusulas abusivas ou impostas no fornecimento de produtos e serviços;

Vale ressaltar que a responsabilidade da ré é objetiva considerando a relação consumerista entre as partes conforme o disposto no art. 14, *caput*, do CDC o qual assevera que aquele que fornece serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos". Também pelo art. 45 da LGPD que corrobora que "as hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente".

Sendo a responsabilidade objetiva, não há suporte para se inquirir a existência de culpa ou a presença de suas modalidades (imperícia, negligência ou imprudência). O que ensejou na condenação em razão do ato ilícito relativo ao acesso de dados titularizados pelo autor a terceiros, ocorrendo a violação a direitos de personalidade (intimidade, privacidade, nome).

A sentença determinou que a empresa não repassasse ou concedesse dados pessoais, financeiros ou sensíveis do cliente a terceiros, sob pena de multa de R$ 300 por contato indevido e ao pagamento a título de dano moral no importe de R$ 10.000,00 nos termos do artigo 944 do Código Civil, ou seja, pela extensão do dano causado.

Além deste acontecido, há outro caso de relevante apreciação da qual rendeu um julgamento pelo plenário do Supremo Tribunal Federal (STF) que solidificou o direito à privacidade como um direito fundamental na Constituição da República Federativa do Brasil.

---

[24] II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

O Plenário do Supremo Tribunal Federal suspendeu a eficácia da Medida Provisória (MP) 954/2020, que previa o compartilhamento de dados de usuários de telecomunicações com o Instituto Brasileiro de Geografia e Estatística (IBGE) para a produção de estatística oficial durante a pandemia do novo coronavírus, ou seja, a realização de entrevistas em caráter não presencial no âmbito de pesquisas domiciliares.

A norma obrigava que as empresas de telefonia disponibilizassem ao IBGE a relação de nomes, números de telefones e os respectivos endereços, tanto de pessoas físicas quanto de pessoas jurídicas.

As cinco Ações Diretas de Inconstitucionalidade[25] alegavam que a MP, ao obrigar as empresas de telefonia fixa e móvel a disponibilizar ao IBGE a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas, violaria os dispositivos da Constituição Federal que asseguram a dignidade da pessoa humana, a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas e o sigilo dos dados.

É notório que essas ações afetam os dados pessoais, que lhe concernem, fragmenta o direito a intimidade que é componente intrínseco a formação do indivíduo e seu modo de ser, revelando um prisma que define propriamente cada uma das pessoas que compõem a população brasileira, colidindo-se aos direitos da personalidade.

Além disso, os impactos se expandem por trazerem elementos da vida particular, que se define pelas informações que o titular pode escolher se serão expostas ou não, bem como os indivíduos que poderão ter acesso a esta informação, o que não ocorreu na medida legislativa atípica, considerando que os dados de todos os indivíduos são invioláveis.

Apesar de violar os direitos fundamentais, a medida se choca com a Lei Geral de Proteção de Dados, que embora ainda seja incapaz de aplicar suas sanções, já está em vigor e serve como guia às diretrizes de dados coletados e compartilhados.

Por maioria de votos, foram referendadas medidas cautelares deferidas pela ministra Rosa Weber nessas Ações Diretas de Inconstitucionalidade (ADIs) para

---

[25] ADI 6387, ADI 6388, ADI 6389, ADI 6390 e ADI 6393

firmar o entendimento de que o compartilhamento previsto na MP viola o direito constitucional à intimidade, à vida privada e ao sigilo de dados.

Tais informações, relacionadas à identificação – efetiva ou potencial – de pessoa natural, configuram dados pessoais e integram, nessa medida, o âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, *caput*)[26], da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII)[27].

Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II[28], da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais. Desse modo, sua manipulação e tratamento, haveria de observar, sob pena de lesão a esses direitos, os limites delineados pela proteção constitucional.

Um trecho do voto da relatora ministra Rosa Weber explicita corretamente este entendimento:

> Não estou a afirmar que de modo algum os dados objeto da **Medida Provisória nº 954/2020** possam ser compartilhados com o IBGE. O que explicito, neste juízo perfunctório, é que **não se pode fazê-lo de uma forma que não garanta mecanismos de proteção compatíveis com as cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, *caput*), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII).** (grifo do autor). (ADI 6387/DF, Relatora Ministra Rosa Weber, Tribunal Pleno, julgado em 07/05/2020).

Assim o Tribunal, por maioria, referendou a medida cautelar deferida para suspender a eficácia da Medida Provisória nº 954/2020, vencido o voto do Ministro Marco Aurélio.

Diante do exposto, depreende-se que a Lei Geral de Proteção de Dados já se mostra como parâmetro para os casos apresentados de violação e compartilhamento

---

[26] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...)

[27] X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

[28] I - o respeito à privacidade; II - a autodeterminação informativa;

irregular de dados, impondo-se como o instrumento legal para proteger, preservar e evitar irregularidades no tratamento de dados pessoais coletados.

CONCLUSÃO

Uma vez que os utilizadores frequentemente têm pouco controle sobre o uso subsequente das informações que concedem, muita da responsabilidade pelo seu uso apropriado recai sobre o responsável pelo tratamento, ou seja, aquele que coleta e os trata.

Assim, as organizações precisam se adaptar à Lei Geral de Proteção de Dados, uma vez que compartilham irregularmente ou cometem vazamentos de dados, ainda que de forma acidental, estarão sujeitas a diversas penalidades, tanto da Lei supracitada quanto de outras normas vigentes.

Deste modo, preliminarmente as empresas que coletam e armazenam essas informações devem implementar a LGPD, através de um fluxo de medidas contidas nela, com o intuito de evitar o compartilhamento irregular destas bases de conhecimento e rever sua política de segurança da informação, como também adequando-os, sejam eles dados pessoais sensíveis ou de crianças e adolescentes, às suas especificidades, respeitando os princípios da LGPD.

Inconcebível enxergar a proteção desses conteúdos como mero ato dispendioso, ao invés de um investimento necessário e capaz de transmitir para o titular a preocupação dos agentes de tratamento para com eles, em razão de sua privacidade e segurança.

Portanto, as sanções administrativas, a responsabilidade e ressarcimento de danos a partir da falta de segurança da informação e compartilhamento irregular de dados, são os instrumentos aditados pelo legislador brasileiro através do ordenamento pátrio e da LGPD, com o intuito de encorajar uma cultura de ética e baseada desde a concepção nas normas vigentes, assegurando que os prestadores de serviço estão cientes das escolhas desde a concepção que integram a privacidade e outros princípios éticos nos produtos e serviços que tratam desses elementos pessoais.

Deste modo, o presente projeto de pesquisa demonstrou contundentemente que é necessária uma legislação referente à proteção de dessas informações pessoais, não o bastante, que também é imprescindível a adequação e aplicação correta de suas sanções ante o cenário brasileiro.

Nesse sentido, expande-se o entendimento da teoria da privacidade em contexto para essa análise, o que enseja uma assimilação da contextualização social

de cada caso, bem como a maleabilidade da privacidade em torno da compreensão da coleta, tratamento e uso dos materiais pessoais recolhidos.

Resta-se categoricamente demonstrado o avanço impulsionado pela LGPD, haja vista que o Brasil é um dos países mais propenso a sofrer vazamentos de dados em todo o mundo. Com a LGPD vigente, os dados pessoais encontram um novo patamar de segurança, a julgar pela efetivação do direito à privacidade pelo STF, pela adoção a título de orientação nos casos recentes e do eminente emprego de suas sanções a partir de 1º de agosto de 2021.

Enfim, observa-se que a Lei Geral de Proteção de Dados já se mostra como referência para os casos apresentados de violação e compartilhamento irregular de dados, caracterizando-se como o instrumento legal para proteger, preservar e evitar irregularidades dos elementos individuais colhidos dos usuários, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural no ordenamento pátrio.

REFERÊNCIAS

ARTHUR, Charles. **Tech giants may be huge, but nothing matches big data**. *The Guardian.* Disponível em: https://www.theguardian.com/technology/2013/aug/23/tech-giants-data. Acesso em: 1 fev. 2021.

AYRES, M. M. T. **LEI GERAL DE PROTEÇÃO DE DADOS: A AUTODETERMINAÇÃO INFORMACIONAL E SEUS DESAFIOS**. Revista Intraciência, Guarujá-SP, Ed. n. 18. Disponível em: https://uniesp.edu.br /sites/guaruja/exibe_edicao.php?id_edicao=282. Acesso em: 20 abr. 2021.

BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. **Cadernos Jurídicos**, São Paulo, v. 1, n. 53, p. 191-201, mar./2020. Disponível em:https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ ii_9_anonimização_e_dado.pdf. Acesso em: 8 mar. 2021.

BIONI, Bruno Ricardo. **Proteção de dados Pessoais** – A Função e os Limites do Consentimento. Rio de janeiro, Ed. Forense, 1ª Ed, 2019.

BIONI, Bruno Ricardo. **Proteção de dados Pessoais** – A Função e os Limites do Consentimento. Rio de janeiro, Ed. Forense, 2ª Ed, 2020.

BRASIL. [Constituição (1946)]. Constituição dos Estados Unidos do Brasil (de 18 de setembro de 1946). Rio de Janeiro, RJ: Presidente [1946]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao46.htm. Acesso em: 11 abr. 2021.

BRASIL. [Constituição (1967)]. Constituição da República Federativa do Brasil de 1967. Brasília, DF: Mesas das Casas do Congresso Nacional [1967]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao67.htm. Acesso em: 11 abr. 2021.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República [2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 11 abr. 2021.

BRASIL. Código Civil. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Brasília, DF: Presidência da República [2002]. República Federativa do Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 12 abr. 2021.

BRASIL. Código de Defesa do Consumidor. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República [1990]. República Federativa do Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 11 abr. 2021.

BRASIL. **Constituição de 1946.** Disponível em: http://www2.camara.leg.br/legin/fed/consti/1940-1949/constituicao-1946-18-julho-1946-365199-publicacaooriginal-1-pl.html. Acesso em: 09 nov. 2020.

BRASIL. **Constituição de 1967**. Disponível em: http://www2.camara.leg.br/legin/fed/consti/1960-1969/constituicao-1967-24-janeiro-1967-365194-publicacaooriginal-1-pl.html. Acesso em: 10 nov. 2020.

BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD). Lei nº 13.709, de 14 de agosto de 2018. Brasília, DF: Presidência da República [2018]. República Federativa do Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 11 abr. 2021.

BRASIL. Marco Civil da Internet. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República [2014]. República Federativa do Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 abr. 2021.

BRASIL. MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS. Unidade Especial de Proteção de Dados e Inteligência Artificial – ESPEC. TERMO DE AJUSTAMENTO DE CONDUTA: TAC n. 01/2019 - ESPEC. Inquérito Civil Público n º 08190.044813/18-44. Promotor de Justiça Frederico Meinberg Ceroy. 16 jan. 2019. Disponível em: https://www.mpdft.mp.br/portal/pdf/tacs/espec/TAC_Espec_2019_001.pdf. Acesso em: 10 abr. 2021.

BRASIL. Superior Tribunal de Justiça. Súmula 297. Disponível em: https://scon.stj.jus.br/docs_internet/VerbetesSTJ.pdf. Acesso em: 10 abr. 2021.

BRASIL. Superior Tribunal de Justiça. Súmula 479. Disponível em: https://scon.stj.jus.br/docs_internet/VerbetesSTJ.pdf. Acesso em: 10 abr. 2021.

BRASIL. Supremo Tribunal Federal. Plenário. ADI 6387/DF, Relatora Ministra Rosa Weber, julgado em 07/05/2020. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165. Acesso em: 12 abr. 2021

BRASIL. TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS. AUDIÊNCIA DE CONCILIAÇÃO: 0721831-64.2018.8.07.0001. 15ª Vara Cível da Circunscrição Especial Judiciária de Brasília. Juiz João Luis Zorzo. 18 dez. 2018. Disponível em: https://www.mpdft.mp.br/portal/pdf/noticias/dezembro_2018/Ata_de_Audiência_Banco_Inter.pdf. Acesso em: 10 abr. 2021.

BRASIL. TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO. SENTENÇA: 1080233-94.2019.8.26.0100. Foro Central Cível. 13ª Vara Cível. Juíza Tonia Yuka Koroku. 29 set. 2020. Disponível em: https://www.conjur.com.br/dl/compartilhar-dados-consumidor-terceiros.pdf. Acesso em: 25 mar. 2021.

CAMAROTTO, Murillo. **Uso de empresas de fachada para venda ilegal de dados entra na mira do governo**. *Valor Econômico*. Disponível em:

https://valor.globo.com/brasil/noticia/2020/09/24/uso-de-empresas-de-fechada-para-venda-ilegal-de-dados-entra-na-mira-do-governo.ghtml. Acesso em: 4 mar. 2021.

CANALTECH. **O que é DoS e DDoS?**. Disponível em: https://canaltech.com.br/produtos/o-que-e-dos-e-ddos/. Acesso em: 12 mar. 2021.

CANOTILHO, José Joaquim Gomes. **Direito Constitucional**. Coimbra: Almedina, 2003.

CARDOSO, Letycia. **Vazamento de dados: Brasil é o país com mais informações roubadas de cartões**. *Jornal O Globo*. Disponível em: https://oglobo.globo.com/economia/defesa-do-consumidor/vazamento-de-dados-brasil-o-pais-com-mais-informacoes-roubadas-de-cartoes-24862696. Acesso em: 3 mar. 2021.

CARVALHO, Kildare Gonçalves. **Direito Constitucional. 15. ed., rev. atual. e ampl.** Belo Horizonte: Del Rey, 2009.

CEGŁOWSKI, Maciej. **The New Wilderness**. *Idle Words*. Disponível em: https://idlewords.com/2019/06/the_new_wilderness.htm. Acesso em: 20 abr. 2021.

COLOMBO, Cristiano. **Antecedentes históricos sobre o direito de privacidade no direito brasileiro**. *Direito & TI*. Disponível em: http://direitoeti.com.br/artigos/antecedentes-historicos-sobre-o-direito-de-privacidade-no-direito-brasileiro/. Acesso em: 25 abr. 2021.

CUNHA JÚNIOR. Dirley**. Curso de Direito Constitucional. 12. ed., rev. ampl. e atual.** Bahia: JusPODIVM, 2018.

DA HORA, Nina. **A corrida da segurança da informação sem os corredores principais**. *MIT Technology Review.* Disponível em: https://mittechreview.com.br/a-corrida-da-seguranca-da-informacao-sem-os-corredores-principais/. Acesso em: 8 mar. 2021.

DE LIMA, C. F. **O *PROFILING* E A PROTEÇÃO DE DADOS PESSOAIS**. Disponível em: http://hdl.handle.net/10183/199951. Acesso em: 19 abr. 2021.

DE MORAES, Mirtes. O Brasil (não é) para principiantes. **Anais eletrônicos do XXII Encontro Estadual de História da ANPUH-SP Santos-2014**, Santos, v. 1, n. 1, p. 1-14, set./2014. Disponível em: http://www.encontro2014.sp.anpuh.org/resources/anais/29/1409167372_ARQUIVO_ANPUH-CONGRESSO.pdf. Acesso em: 12 mar. 2021.

DECEW, JUDITH, "Privacy", **The Stanford Encyclopedia of Philosophy (Spring 2018 Edition), Edward N. Zalta (ed.),** Disponível em: https://plato.stanford.edu/archives/spr2018/entries/privacy/. Acesso em: 7 nov. 2020.

DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia**. Escola Nacional de Defesa do Consumidor, Brasília-

DF, v. 2, p. 69, 2010. Disponível em: https://www.justica.gov.br/seus-direitos/consumidor/Anexos/manual-de-protecao-de-dados-pessoais.pdf. Acesso em: 20 abr. 2021.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico Journal of Law [EJJL], v. 12 n.2, p. 91-108, 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 21 abr. 2021.

ESPAÑA. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Artículos 72, 73 y 74. Madrid, ES: Presidente del Gobierno [2018]. Disponível em: https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673 Acesso em: 11 abr. 2021.

FERREIRA, Giovana; FERREIRA, Fernanda; DO CARMO, E. F. **O dilema entre a garantia da liberdade de expressão e o direito à privacidade no marco civil da internet: uma análise da Lei nº 12.965, de 23 de abril de 2014**. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 20, n. 4303, 13 abr. 2015. Disponível em: https://jus.com.br/artigos/37886. Acesso em: 20 abr. 2021.

FIEGO, Lívia. **Os desafios da Lei Geral de Proteção de Dados no atendimento ao cliente**. *Estadão*. Disponível em: https://politica.estadao.com.br/blogs/fausto-macedo/os-desafios-da-lei-geral-de-protecao-de-dados-no-atendimento-ao-cliente/. Acesso em: 20 abr. 2021.

FLORENÇO, Larissa Britto. **A PROTEÇÃO DE DADOS PESSOAIS NAS RELAÇÕES DE CONSUMO COMO UM DIREITO FUNDAMENTAL: PERSPECTIVAS DE UM MARCO REGULATÓRIO PARA O BRASIL**. Revista da ESMESC, Florianópolis-SC, v. 23, n. 29, p. 165-182, mar./2016. Disponível em: https://revista.esmesc.org.br/re/article/view/144. Acesso em: 20 abr. 2021.

G1. **Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber**. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml. Acesso em: 12 mar. 2021.

GHEDIN, Rodrigo. **Independente e livre de Facebook e Google: este é o novo Manual do Usuário**. *Manual do Usuário*. Disponível em: https://manualdousuario.net/manual-terceira-fase/. Acesso em: 8 mar. 2021.

GOULART, Guilherme Damasio. **Condicionamento, liberdade e privacidade: compreendendo as novas tecnologias por meio do admirável mundo novo**. Revista Diálogos do Direito, v.4, n. 6, julho de 2014. Disponível em: http://ojs.cesuca.edu.br/index.php/dialogosdodireito/article/view/580. Acesso em: 10 nov 2020.

GOVERNO FEDERAL - GOVERNO DO BRASIL. **Guia de Boas Práticas - Lei Geral de Proteção de Dados (LGPD)**. Disponível em: https://www.gov.br/governodigital/pt-

br/governanca-de-dados/guia-de-boas-praticas-lei-geral-de-protecao-de-dados-lgpd. Acesso em: 4 mar. 2021.

Griswold v. Connecticut, 381 U.S. 479 (1965). Disponível em: https://supreme.justia.com/cases/federal/us/381/479/. Acesso em: 10 Nov 2020.

Griswold v. Connecticut, 381 US 479 - Supreme Court 1965. Disponível em: https://scholar.google.com/scholar_case?case=12276922145000050979&q=Griswold+v.+Connecticut&hl=en&as_sdt=2006. Acesso em: 10 Nov 2020.

GRÖNE, Florian, PÉLADEAU, Pierre, SAMAD, Rawia Abdel. **Tomorrow's data heroes**. *Strategy+Business.* Disponível em: ht https://www.strategy-business.com/article/Tomorrows-Data-Heroes. Acesso em: 19 abr. 2021.

GUIA DA CARREIRA. **Saiba tudo sobre a faculdade de Marketing e veja onde cursar**. Disponível em: https://www.guiadacarreira.com.br/cursos/faculdade-de-marketing/. Acesso em: 24 mar. 2021.

HELP DIGITAL. **O que é firewall? – Conceito, tipos e arquiteturas**. Disponível em: https://helpdigitalti.com.br/o-que-e-firewall-conceito-tipos-e-arquiteturas/. Acesso em: 12 mar. 2021.

IBM SECURITY. **Cost of a Data Breach Report de 2020**. Disponível em: https://www.ibm.com/br-pt/security/data-breach. Acesso em: 3 mar. 2021.

INDIANA UNIVERSITY. **What are cookies?**. Disponível em: https://kb.iu.edu/d/agwm. Acesso em: 24 fev. 2021.

INTLX SOLUTIONS, LLC. **2018 Cost of a Data Breach Study: Benchmark research sponsored by IBM Security Independently conducted by Ponemon Institute LLC Global Overview**. Disponível em: https://www.intlxsolutions.com/hubfs/2018_Global_Cost_of_a_Data_Breach_Report.pdf. Acesso em: 20 out. 2020.

ISTOÉ. **Banco Inter nega vazamento de informações de clientes**. Disponível em: https://istoe.com.br/banco-inter-nega-vazamento-de-informacoes-de-clientes/.Acesso em: 12 abr. 2021.

KEMP, Simon. **DIGITAL 2020: BRAZIL**. *Datareportal - Global Digital Insights.* Disponível em: https://datareportal.com/reports/digital-2020-brazil. Acesso em: 2 mar. 2021.

LAGO, F. W. G. D; REIS, J. M. O. D. SOCIEDADE DE CONSUMIDORES NA VISÃO DE BAUMAN E DRUMMOND: interdiscursividade nas obras dos autores. **Cadernos Zygmunt Bauman**, São Luís-MA, v. 6, n. 12, p. 39-50, jan./2017. Disponível em: http://www.periodicoseletronicos.ufma.br/index.php/bauman/issue/view/394. Acesso em: 24 mar. 2021.

MCGEE, Bill. **Do travel deals change based on your browsing history?**. USA TODAY. Disponível em: https://www.usatoday.com/story/travel/columnist/mcgee/

2013/04/03/do-travel-deals-change-based-on-your-browsing-history/2021993/. Acesso em: 24 mar. 2021.

MIT TECNOLOGY REVIEW. **Cookie statement**. Disponível em: https://www.technologyreview.com/cookies/. Acesso em: 24 fev. 2021.

MPDFT. **Banco Inter: acordo destinará R$ 1,5 milhão para caridade e combate a crimes cibernéticos**. Disponível em: https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2018/10524-2018-12-19-10-27-31. Acesso em: 12 abr. 2021.

MPDFT. **Caso Netshoes: clientes afetados em vazamento de dados serão comunicados**. Disponível em: https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2018/9821-caso-netshoes-clientes-afetados-em-vazamento-de-dados-serao-comunicados. Acesso em: 11 abr. 2021.

MPDFT. **MPDFT ajuíza 1ª ação civil pública com base na LGPD**. Disponível em: https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2020/12384-mpdft-ajuiza-1-acao-civil-publica-com-base-na-lgpd. Acesso em: 22 fev. 2021.

MPDFT. **MPDFT ajuíza ação contra o Banco Inter por vazamento de dados pessoais**. Disponível em: https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2018/10211-mpdft-ajuiza-acao-contra-o-banco-inter-por-vazamento-de-dados-pessoais. Acesso em: 12 abr. 2021.

MPDFT. **MPDFT e Netshoes firmam acordo para pagamento de danos morais após vazamento de dados**. Disponível em: https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2019/10570-mpdft-e-netshoes-firmam-acordo-para-pagamento-de-danos-morais-coletivos-apos-vazamento-de-dados. Acesso em: 12 abr. 2021.

MPDFT. **MPDFT obtém decisão que suspende a venda de dados pessoais pela Serasa Experian**. Disponível em: https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2020/12586-mpdft-obtem-decisao-que-suspende-a-venda-de-dados-pessoais-pela-serasa-experian. Acesso em: 24 mar. 2021.

NETO, A. P. S. Superendividamento do consumidor: Conceito, Pressupostos e Classificação. **Revista da SJRJ**, Rio de Janeiro, v. 1, n. 26, p. 167-184, dez./2009. Disponível em: https://www.jfrj.jus.br/sites/default/files/revista-sjrj/arquivo/36-153-1-pb.pdf. Acesso em: 1 mar. 2021.

NISSENBAUM, Helen. **Privacy in context: technology, policy, and the integrity of social life**. Stanford: Stanford University Press, 2010, p. 231, tradução livre.

OLIVEIRA, Moacyr de. **“Intimidade”, in Enciclopédia Saraiva do Direito. In SILVA, José Afonso da. Curso de direito constitucional positivo**. 19. ed. rev. e atual. São Paulo: Malheiros Editores, 2001.

OLIVEIRA, Regiane; ROSSI, Marina. **No submundo da internet, prospera o lucrativo negócio de chantagear empresas em meio à pandemia**. *EL PAÍS Brasil*. Disponível em: https://brasil.elpais.com/tecnologia/2020-07-03/no-submundo-da-internet-prospera-o-lucrativo-negocio-de-chantagear-empresas-em-meio-a-pandemia.html. Acesso em: 24 mar. 2021.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais**: Comentários à Lei n. 13.709/2018. São José dos Campos - SP, Ed. Saraiva Jur, 1ª Ed, 2018.

PODESTÁ, Fábio Henrique. **Direito à intimidade em ambiente da internet.** In: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coords.). Direito & Internet: aspectos jurídicos relevantes: São Paulo: Quarter Latin, 2005.

SALESFORCE. **Predictive Marketing & Why You Should Look Into It**. Disponível em: https://www.salesforce.com/products/marketing-cloud/best-practices/predictive-marketing/. Acesso em: 24 mar. 2021.

SERPRO. **O que muda com a LGPD**. Disponível em: https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd. Acesso em: 20 abr. 2021.

SILVA, José Afonso da Silva**, Curso de Direito Constitucional Positivo**, 19ª ed., São Paulo: Malheiros, 1997.

SOLON, Olivia. **Facebook says Cambridge Analytica may have gained 37m more users' data**. *The Guardian*. Disponível em: https://www.theguardian.com/technology/2018/apr/04/facebook-cambridge-analytica-user-data-latest-more-than-thought. Acesso em: 10 abr. 2021.

SOPRANA, Paula. **Política de privacidade do WhatsApp é questionada no Ministério da Justiça e na ANPD**. *Folha de S.Paulo*. Disponível em: https://www1.folha.uol.com.br/mercado/2021/04/privacidade-do-whatsapp-e-questionada-no-ministerio-da-justica-e-na-anpd.shtml/. Acesso em: 30 abr. 2021.

SOUTO, Sabine Müller; MACHADO, Maykon Fagundes. **LGPD e a nova política de privacidade dos dados do WhatsApp**. *Conjur*. Disponível em: https://www.conjur.com.br/2021-jan-20/opiniao-lgpd-politica-privacidade-whatsapp. Acesso em: 19 abr. 2021.

SUPREMO TRIBUNAL FEDERAL. **STF suspende compartilhamento de dados de usuários de telefônicas com IBGE**. Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=442902. Acesso em: 12 abr. 2021.

TEIXEIRA, Fernando. **Como o Marketing Preditivo está mudando a compra de mídia e a propaganda digital**. *MIT Technology Review.* Disponível em:

https://mittechreview.com.br/como-o-marketing-preditivo-esta-mudando-a-compra-de-midia-e-a-propaganda-digital/. Acesso em: 9 fev. 2021.

TEXAS TECH UNIVERSITY. **Scams – Spam, Phishing, Spoofing and Pharming**. Disponível em: https://www.ttu.edu/cybersecurity/lubbock/digital-life/digital-identity/scams-spam-phishing-spoofing-pharming.php. Acesso em: 15 fev. 2021.

TOMASEVICIUS FILHO, Eduardo. **Marco Civil da Internet: uma lei sem conteúdo normativo**. Estudos Avançados. São Paulo-SP, v. 30, n.86, 269-285, 2016. Disponível em: https://www.revistas.usp.br/eav/article/view/115093. Acesso em: 20 abr. 2021.

UOL. **Brasil é o segundo país no mundo com maior número de crimes cibernéticos**. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2018/02/15/brasil-e-o-segundo-pais-no-mundo-com-maior-numero-de-crimes-ciberneticos.htm. Acesso em: 24 mar. 2021.

VENTURA, Felipe. **Netshoes paga R$ 500 mil em danos morais após vazamento de dados**. *Tecnoblog*. Disponível em: https://tecnoblog.net/277594/netshoes-acordo-mpdft-vazamento-dados/. Acesso em: 11 abr. 2021.

WARREN, S.D., BRANDEIS, L.D.: **The Right to Privacy. Harvard Law Review. Vol. IV**. December 15, 1890. Disponível em: https://www.jstor.org/stable/1321160. Acesso em: 7 nov. 2020.

WHATSAPP. **Política de Privacidade - fevereiro 2021**. Disponível em: https://www.whatsapp.com/legal/updates/privacy-policy?lang=pt_br. Acesso em: 8 fev. 2021.

WIKIPÉDIA. **Big data**. Disponível em: https://pt.wikipedia.org/wiki/Big_data. Acesso em: 24 mar. 2021.

ZANINI, Leonardo Estevam de Assis. **O surgimento e o desenvolvimento do right of privacy nos Estados Unidos.** Revista de Doutrina da 4ª Região, Porto Alegre, n.64, fev. 2015. Disponível em: http://ajufe.org.br/images/bkp/ajufe/arquivos/downloads/leonardo-estevam-de-assis-zanini-o-surgimento-e-o-desenvolvimento-do-right-of-privacy-nos-estados-unidos-2661518.pdf. Acesso em: 09 nov. 2020.