UNIVERSIDADE DO VALE DO RIO DOS SINOS – UNISINOS
UNIDADE ACADÊMICA DE PESQUISA E PÓS-GRADUACÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
NÍVEL MESTRADO PROFISSIONAL

TIAGO VINÍCIUS SOARES SILVA

O TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS NAS EMPRESAS DO SETOR DA SAÚDE, SEGUNDO A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Porto Alegre
2020

TIAGO VINÍCIUS SOARES SILVA

O TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS NAS EMPRESAS DO SETOR DA SAÚDE, SEGUNDO A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Dissertação apresentada como requisito parcial para a obtenção do título de Mestre em Direito da Empresa, pelo programa de Pós-Graduação em Direito da Universidade do Vale do Rio dos Sinos – UNISINOS.

Orientador: Prof.Dr. Fabiano Koff Coulon

Porto Alegre

2020

S586t Silva, Tiago Vinícius Soares
O tratamento de dados pessoais sensíveis nas empresas do setor da saúde, segundo a Lei Geral de Proteção de Dados (LGPD) / por Tiago Vinícius Soares Silva. – 2020.

128 f. : 30 cm.

Dissertação (mestrado) — Universidade do Vale do Rio dos Sinos, Programa de Pós-Graduação em Direito, 2020.

Orientação: Prof. Dr. Fabiano Koff Coulon.

1. LGPD. 2. Tratamento de dados. 3. Dados sensíveis. 4. Compliance. 5. Caldicott. I. Título.

Catalogação na Fonte:
Bibliotecária Vanessa Borges Nunes - CRB 10/1556

1 UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS
UNIDADE ACADÊMICA DE PESQUISA E PÓS-GRADUAÇÃO

PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO DA EMPRESA E DOS NEGÓCIOS NÍVEL MESTRADO PROFISSIONAL

O Trabalho de Conclusão de Curso intitulado: "**O TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS NAS EMPRESAS DO SETOR DA SAÚDE, SEGUNDO A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)",** elaborado pelo mestrando **Tiago Vinicius Soares,** foi julgado adequado e aprovado por todos os membros da Banca Examinadora para a obtenção do título de MESTRE EM DIREITO DA EMPRESA E DOS NEGÓCIOS - Profissional.

Porto Alegre, 15 de setembro de 2020.

(Participação por webconferência) Prof. Dr. **Wilson Engelmann**

Coordenador do Programa de Mestrado Profissional em Direito da Empresa e dos Negócios

Apresentada à Banca integrada pelos seguintes professores:

Presidente: Dr. Fabiano Koff Coulon (Participação por webconferência)

Membro: Dr. Cristiano Colombo (Participação por webconferência)

Membro: Dr. Wilson Engelmann (Participação por webconferência)

Membro Externo: Dr. Rafael Dresch (Participação por webconferência)

À Ele, que me encontrou quando eu estava perdido.

AGRADECIMENTOS

Agradecer nem sempre envolve justiça, por sempre se deixar alguém que foi fundamental sem os devidos créditos. Minhas desculpas desde já.

Gostaria de agradecer, primeiro, à Deus, pelo dom da vida.

Em seguida, agradeço a UNISINOS, por ter acreditado no projeto do mestrado profissional no Juazeiro-CE, vindo suprir uma grande lacuna acadêmica na região.

Meus sinceros agradecimentos ao prof. Dr. Fabiano Coulon, por ter sido um orientador primoroso e dedicado, me passando a segurança de que meu trabalho estava de fato sendo levado à sério por alguém de maior gabarito que o meu.

Agradeço, também, ao prof. Dr. Wilson, que foi como um segundo orientador, usando sua paixão pela pesquisa como um propulsor para não me deixar desistir.

Agradeço, em especial, à minha esposa, Gláucia, que no início do mestrado era namorada, no curso, noiva, e agora, no final dessa jornada, uma esposa que além de me permitir ser padrasto de Vinícius, que por sua beleza de espírito dispensa comentários, acredita mais em mim do que eu mesmo.

Aos meus queridos pais, Ednaldo e Valdicleide, que sempre abraçaram meus projetos com uma fé inabalável de que no final daria tudo certo.

Aos meus irmãos, Isaac e Guilherme, os quais, mesmo que eu não entenda os motivos, veem em mim um referencial, e para o bem da verdade, ocorre o inverso.

Aos amigos e colegas que, direta ou indiretamente, me ajudaram nesse projeto de vida, meus sinceros agradecimentos.

Uma máquina pode fazer o trabalho de cinquenta pessoas comuns. Nenhuma máquina pode fazer o trabalho de uma pessoa extraordinária.

Elbert Hubbard

RESUMO

Segundo a pesquisa "*The end of the beginning – Unleashing the transformational power of GDPR"*, realizada em 2018, 60% das empresas já adotam a regulamentação de tratamento de dados da União Europeia. No Brasil, a previsão é que em 2020 entre em vigor a Lei Geral de Proteção de Dados (LGPD), mundando, totalmente, o cenário de tratamento de dados no país. O presente estudo tem como objetivo examinar as exigências legais trazidas pela LGPD às empresas de saúde, de modo a delinear procedimentos e opções práticas de compliance à implementação do tratamento de dados sensíveis na sua nova realidade e inviabilizar, ao máximo, as multas administrativas contra este tipo de empresas. O problema da pesquisa tenta responder a seguinte questão: quais pilares do compliance poderão ser estruturados nas empresas do setor da saúde para que se adaptem ao tratamento de dados pessoais sensíveis, segundo a LGPD? Para se chegar nessa resposta, foi tratado no primeiro capítulo sobre a importância econômica dos dados sensíveis no cenário mundial e nacional, justificando a necessidade da criação de uma regulamentação de proteção de dados pessoais de clientes/consumidores. Em sequência, no segundo capítulo, foi feita uma análise técnica sobre a nova regulação de dados da União Europeia com a do Brasil e quais as principais exigências trazidas por esta ao tratamento de dados pessoais sensíveis no cenário das empresas de saúde. No terceiro capítulo, se buscou apontar o compliance como possível estratégia de adaptação das empresas do setor da saúde à nova realidade que se avizinha. Como metodologia de pesquisa, esse trabalho se valeu da abordagem qualitativa, com procedimentos de pesquisa bibliográfica, de legislações internacionais e nacionais, estatísticas já documentadas, livros, periódicos científicos e rede de internet, unindo a isso a natureza de pesquisa aplicada, com a entrega de um Termo de Consentimento de Uso de Dados. No final, se concluiu que o programa de compliance, com especial atenção ao código de conduta e ao código de ética, se valendo dos princípios de Caldicott, é uma ferramenta muito útil para suprir as exigências legais trazidas pela nova legislação às empresas brasileiras do setor da saúde.

Palavras-chave: LGPD. Tratamento de dados. Dados sensíveis. Compliance. Caldicott.

ABSTRACT

According to the survey “The end of the beginning - Unleashing the transformational power of GDPR”, carried out in 2018, 60% of companies have already adopted data processing in the European Union. In Brazil, the forecast is that in 2020 the General Data Protection Law (GDPL) will come into effect, totally changing the scenario of data processing in the country. The present study aims to examine the legal requirements brought by GDPL to healthcare companies, in order to outline procedures and practical options for compliance with the implementation of data processing related to its new reality and make it impossible, as much, as administrative fines against this type of companies. The research problem tries to answer the following question: what are the pillars of compliance that can be structured in companies in the health sector so that they adapt to the treatment of sensitive personal data, according to the GDPL? To arrive at this answer, it was treated in the first chapter on the economic importance of relevant data in the world and national scenario, justifying the need to create a need to protect personal data of customers / consumers. Subsequently, in the second chapter, a technical analysis was made on the new data regulation of the European Union with that of Brazil and what are the main requirements brought to it for the treatment of sensitive personal data in the scenario of healthcare companies. In the third chapter, we sought to point out compliance as a possible strategy for adapting companies in the health sector to the new reality that lies ahead. As a research methodology, this work made use of the qualitative approach, with bibliographic research procedures, international and national legislation, already documented statistics, books, scientific journals and internet network, adding to this the nature of applied research, with the delivery Data Consent Form. Not final, it was concluded that the compliance program, with special attention to the code of conduct and the code of ethics, using the Caldicott principles, is a very useful tool to meet the legal requirements brought by the new legislation to brazilian companies in the sector of health.

Keywords: GDPL. Data processing. Sensitive data. Compliance. Caldicott.

SUMÁRIO

2 INTRODUÇÃO

Muito embora a imagem distópica de uma sociedade controlada por forças políticas e econômicas poderosas, ditando a rotina e os hábitos das pessoas, manipulando seus dados e reeditando a história conforme lhes apraz parecesse uma mera ficção distante de George Orwell[1], na sociedade moderna do século XXI, se não no exagero tão comum às distopias, pelo menos na constante integração do homem e máquina se nota alguma semelhança com os cenários traçados para o futuro da humanidade.

Pela primeira vez na história humana o acesso a dados de toda natureza estão literalmente mudando os hábitos das pessoas, principalmente nas relações de consumo, e traçando uma perspectiva de futuro cujo conceito de privacidade poderá ser totalmente flexibilizado nas novas gerações.

É a partir do acesso desses dados, fornecidos pela população diariamente, que as empresas traçam perfis e conduzem os consumidores a consumirem muito mais sem nem saberem que estão sendo induzidos (DUHIGG, 2017, p. 195-225) – o pior ocorre quando esses dados são comercializados sem o conhecimento e autorização prévios do consumidor[2]. Diante disso, literalmente pode-se falar que no século XXI os dados das pessoas valem ouro (HARARI, 2018, p. 106-107).

Em uma tentativa mais incisiva para tentar conter esse fluxo “clandestino” de dados, a União Europeia começou a desenhar regulamentos e diretivas[3] que abriram caminho para a sua GDPR - *General Data Protection Regulation*[4], a qual entrou em vigor no dia 25 de maio de 2018, substituindo a Diretiva 95/46/EC[5], com

---

1 ORWELL, George. **1984**. Tradução Alexandre Hubner e Heloisa Jahn. São Paulo: Companhia das Letras, 2017.

2 Caso do Facebook e Cambridge Analytica. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml>. Acesso em: 18 set. 2020.

3 Diretiva 2016/680: relativa à proteção dos dados destinados às autoridades policiais e judiciárias (Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L0680>. Acesso em: 18 set. 2020.); Regulamento 45/2001: aplicado ao tratamento de dados pessoais por órgãos ou agência da União Europeia (Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32001R0045>. Acesso em: 18 set. 2020.); Diretiva 2000/31: tratando do Comércio Eletrônico (Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32000L0031>. Acesso em: 20 de jun. de 2019.).

4 Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection_en>. Acesso em: 18 set. 2020.

5 Criada em 24 de outubro de 1995. Há de salientar que a internet naquela época era incial, comparada a hoje, não existindo conceitos que hoje são tidos como comuns, como nuvem,

intuito basilar de regulamentar a privacidade e proteção dos dados pessoais e o uso desses dados por terceiros.

Essa necessidade de controle dos dados está sendo algo tão latente no mundo que desde a entrada em vigor da GDPR 117 países já promulgaram as suas respectivas regulamentações e 40 países estão ou em projeto de lei ou em trâmite de aprovação.[6]

Segundo a pesquisa "*The end of the beginning – Unleashing the transformational power of GDPR"*, realizada pela International Business Machines Corporation-IBM em maio de 2018[7], abordando 1.500 líderes de negócios, em 34 países, 60% das empresas já estão adotando a regulamentação da União Europeia como uma oportunidade de aperfeiçoamento de assuntos relacionados à segurança e gerenciamento de dados, privacidade e novos horizontes para os negócios, aos invés de a verem como um impedimento ou obstáculo ao desenvolvimento econômico das empresas.

Seguindo a mesma lógica do restante do mundo, mas em certa medida já tendo se antecipado em alguns aspectos, o Brasil também mirou na necessidade da criação das regulamentações sobre o tema. Desde 2014 o chamado Marco Civil da Internet[8] (Lei n. 12.965/14), o qual estabelecia diretrizes básicas para o uso da Internet, vinha sendo a principal legislação sobre o assunto no Brasil. Não sendo suficiente, ante os crescentes escândalos com impacto mundial que apareciam (Facebook e Cambridge Analytica, por exemplo), fora promulgada, em 15/08/2018, a Lei nº 13.709, chamada de Lei Geral de Proteção de Dados Pessoais, dispondo sobre a proteção de dados pessoais e alterando a lei do Marco Civil da Internet e se tornando tanto a principal lei brasileira, quanto o ponto de convergência com as regulações europeias.[9]

Oficialmente, a nova lei geral entrou em vigor em 18 de setembro de 2020[10], e vai exigir das empresas que lidam com dados pessoais dos seus clientes

---

aplicativos e redes sociais. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046>. Acesos em: 18 set. 2020.

6 Dados colhidos em agosto de 2018, por Danilo Doneda.

7 Disponível em: <https://www.ibm.com/downloads/cas/JEMXN6LV>. Acesso em: 18 set. 2020.

8 Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 18 set. 2020.

9 Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 18 set. 2020.

10 Originalmente a Nova Lei Geral de Proteção de Dados entraria em vigor 18 meses após sua publicação, mas com a Medida Provisória nº 959, de 29 de abril de 2020, o prazo foi estendido eu a *vactio legis* para 3 de maior de 2021 (Disponível em: <http://www.in.gov.br/web/dou/-

adequação aos tratamentos desses dados, sob risco de sofrerem punições que vão desde advertências, multa equivalente a 2% do seu faturamento, limitada ao valor máximo de cinquenta milhões de reais, e multa diária, a ser definida pela autoridade nacional (artigos. 52 a 54).

É certo que cada empresa - e, às vezes, cada setor dentro da própria empresa, deverá buscar sua melhor forma de adaptação, voltando o cumprimento da lei para o seu nicho específico.

Problema maior surge quando se trata dos chamados dados pessoais sensíveis. Segundo o inciso II, do art. 5º, da Lei Geral de Proteção de Dados Pessoais:

> 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;

Para processar todas essas informações, foi criado o chamado “tratamento de dados”, o qual significa, nos termos do art. 5º, X, da LGPD:

> [...] toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Nesse novo cenário global de novas tecnologias, as empresas do setor de saúde brasileiras, principalmente por lidarem com tantos dados potencialmente lesivos à intimidade e a vida privada do cliente/paciente, não terão alternativa senão se adaptarem à essa realidade. Deverão estudar os novos mecanismos de processamento de dados e criarem procedimentos que modernizem seu tratamento de dados pessoais sensíveis.

/medida-provisoria-n-959-de-29-de-abril-de-2020-254499639>. Acesso em: 24 jun. 2020.). No entanto, o Senado Federal havia determinado a sua vigência de forma imediata, e no dia 17/09/2020 o Presidente da República sancionou seu inicío imediato, embora a aplicação das sanções só ocorram a partir de 1 de agosto de 2021. (Disponível em: <https://www.conjur.com.br/2020-set-18/sancao-governo-lgpd-comeca-valer-nesta-sexta>. Acesso em: 18 set. 2020).

Nesse trabalho, irá se analisar as novas diretrizes trazidas pela Lei Geral de Proteção de Dados à tais empresas, principalmente no que diz respeito às novas práticas para o tratamento de dados sensíveis, apontando as consequências primárias do não cumprimento da lei e quais alternativas para se adequar a essa nova realidade. Para tanto, se limitará o objeto da pesquisa tão somente ao Capítulo II da referida lei, o qual aborda o tratamento de dados pessoais, e mais ainda a sua Seção II, a qual traça os requisitos basilares para o tratamento de dados pessoais sensíveis (arts.11 ao 13).

O objetivo geral será examinar as exigências legais trazidas pela LGPD à essas empresas do setor de saúde, de modo a delinear procedimentos e opções práticas de compliance à implementação do tratamento de dados sensíveis (Capítulo II, Seção II, da Lei 13.709 de 14 de agosto de 2018) nas suas novas realidades e inviabilizar, ao máximo, as multas administrativas contra este tipo de empresas. Quanto aos objetivos específicos, tem-se estudar a importância dos dados pessoais no setor da saúde, analisar os requisitos para o tratamento de dados pessoais sensíveis, segundo a Lei Geral de Proteção de Dados (artigos 11 ao 13) e propor um programa de compliance como ferramenta auxiliar às empresas do setor de saúde, integrado e estruturado com os Princípios de Caldicott[11], de modo a realizarem adequadamente o tratamento dos dados sensíveis em nível de qualidade internacional.

Nesse diapasão, no primeiro capítulo será feita uma análise sobre o valor econômico que os dados pessoais possuem no cenário mundial e nacional, trazendo à luz um panorama que possibilitará, e até justificará, a necessidade de regulamentações para tentar inviabilizar não o usufruto econômico dos dados pessoais, mas o uso criminoso e inconsequente deles.

---

[11] Em 1997, diante do alargamento do National Health Service do Reino Unido, foram desenvolvidos seis princípios para a segurança das informações e dados pessoais na área médica, estabelecidos no Relatório Caldicott, encomendado por Dame Fiona Caldicott, a National Data Guardian for health no Reino Unido, recebendo atualização de mais um princípio em abril de 2013, os quais ficaram conhecidos da seguinte forma: 1) Justify the purpose(s) of using confidential information; 2) Only use it when absolutely necessary; 3) Use the minimum that is required; 4) Access should be on a strict need-to-know basis; 5) Everyone must understand his or her responsibilities; 6) Understand and comply with the law; 7) The duty to share information can be as important as the duty to protect patient Confidentiality. Disponível em: <https://www.anahp.com.br/noticias/noticias-do-mercado/a-protecao-de-dados-pessoais-na-area-de-saude/>. Acesso em: 18 set. 2020; Disponível em: <https://www.igt.hscic.gov.uk/Caldicott2Principles.aspx>. Acesso em: 18 set. 2020.

No segundo capítulo será feito um estudo mais detalhado sobre à lei de proteção de dados da União Europeia e sua correlação com à Nova Lei Geral de Proteção de Dados brasileira, apontando que em ambos os casos o surgimentos dessas novas diretrizes legais não foram novidades quando se analisa seus históricos legais sobre o tema.

No último capítulo, se apresentará o compliance como uma ferramenta sólida para ajudar na implementação e manutenção do tratamento de dados pessoais sensíveis nas empresas no setor de saúde, apontando sobre a importância do consentimento do consumidor/paciente para o cumprimento legal, apresentando um formulário de consentimento como opção de ponto de partida na abordagem inicial para com o titular dos referidos dados.

No que diz respeito à própria pesquisa, a abordagem desse trabalho será de uma pesquisa qualitativa, buscando fazer um levantamento da discussão teórica sob os cuidados acima apontados.

Quanto aos procedimentos, serão utilizados a pesquisa bibliográfica, documental, espraiando a produção intelectual mais destacada no momento.

Quanto à natureza da pesquisa, se buscará realizar a modalidade aplicada, com o intuito de gerar conhecimentos para aplicação prática, dirigidos à solução de problemas específicos, de interesse nacional (GERHARDT e SILVERA, 2009, p. 35), findando na entrega de um Termo de Consentimento de Uso de Dados Pessoais e Sensíveis, o qual as empresas do setor de saúde poderão fazer a coleta de dados com as margens estabelecidas pela legislação vigente.

No que diz respeito aos objetivos, esse trabalho focará na pesquisa exploratória, na qual se tem como objetivo “[...] proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a construir hipóteses e identificar os fatos determinantes ou contribuintes a ocorrência dos fenômenos” (GIL, 2007, p. 41).

Dessa maneira, o resultado desse trabalho ajudará as empresas do setor da saúde a entenderem melhor o que seria a operação de tratamento de dados pessoais sensíveis e como realizá-lo na forma da lei com o auxílio de um programa de integridade eficiente.

3 O NOVO CENÁRIO ECONÔMICO MUNDIAL PARA O USO DE DADOS PESSOAIS

O potencial tecnológico e, consequentemente, o econômico que dele deriva, está longe de chegar ao seu ápice de desenvolvimento na era pós-moderna. Mas mesmo assim, não tem havido diminuição no ritmo de avanços de novas tecnologias e de novos meios de aquisições de riquezas.

Nesse novo cenário mundial, muitas facetas de negócios estão aparecendo como algo inovador, tendência do futuro, sendo vendidas como necessidade de adaptação, e não de resistência.

Uma das facetas da revolução que as novas tecnologias e as formas de comunicação estão sofrendo apresenta-se como o processamento de uma quantidade assustadoramente volumosa de dados digitais, os quais atingem proporções em que o ser humano jamais poderia processá-los sem ajuda tecnológica, gerando, com isso, uma codependência humana para com as tecnologias/máquinas. Lippstein (2015, p.3) explica bem essa nova realidade da humanidade:

> A era digital transformou o modo de comportamento do homem, incluiu ferramentas de comunicação sofisticadas, apresentou novos mecanismos de produção, criou aprimorados sistemas de dados, dentre outros. Desenvolveu um mundo, em sua grande parte incorpóreo, mas com capacidade de armazenamento. Essas novas facilidades lograram êxito no século XXI, foram adotadas pelas empresas, pelos governos e mesmo pelos cidadãos comuns, utilizando-se de tais novas ferramentas tanto para benefício pessoal quanto para utilidade profissional.

Esses dados são oriundos da rotina da sociedade moderna, a qual já fez da internet uma parte indispensável do seu cotidiano, estando presente da hora de acordar até a hora de dormir.

Um bom exemplo de aquisição desses dados é explicado por Fernandes e Tambosi (2019, *online*):

> [...] aquele aplicativo que você baixou e dizia ser “gratuito”, na verdade tinha um preço: os seus dados. Informações como hábitos de consumo, questões de interesse, número de documento, contatos e em alguns casos até do cartão de crédito. Hoje essas informações são comercializadas e utilizadas por várias empresas para estimular o consumo de produtos e serviços.

Em contrapartida, imaginar um mundo sem internet pode ser considerado impossível para grande parte das pessoas que lhe faz uso diário. Cada vez mais, como se fosse um poço sem fundo (uma curiosidade compulsiva para descobrir até aonde a tecnologia pode levar a humanidade), tem se exigido mais mudanças e maior rapidez de resposta a cada geração de novos aparelhos eletrônicos que são lançados.

Segundo uma pesquisa do International Business Machines Corporation – IBM (GALINDO, 2016, *online*), realizada em 2013, se constatou que no ano 2000, 25% dos dados já eram digitalizados, no ano de 2007, esse número teve uma evolução mais do que significativa, saltou para 93%, e, por fim, no ano de 2013, chegou no montante impressionante de 98%.

Essa evolução se deu pelo amplo e democrático acesso a dispositivos eletrônicos e a popularização da internet. Com a criação dos aplicativos de facilitação da vida, a dependência do ser humano a tecnologia, principalmente às redes sociais, está muito evidente.

Uma boa análise desse cenário de crescente acessibilidade às redes sociais foi apontada por Keen (2012, p. 39), o qual apresentou os seguintes índices probatórios:

> Como seus membros dedicam mais de 700 bilhões de minutos de seu tempo por mês à rede, o Facebook foi o site mais visitado do mundo em 2010, com 9% de todo tráfego on-line. No começo de 2011, 57% de todos americanos on-line entravam no Facebook pelo menos uma vez por dia; 51% de todos os americanos com mais de doze anos tinham uma conta na rede social; e 38% de todo tráfego de compartilhamento da internet emanavam da criação de Zuckerberg. Em setembro de 2011, mais de 500 milhões de pessoas entravam no Facebook por dia, e seus quase 800 milhões de usuários ativos na época superavam o que era toda a internet em 2004. O Facebook está se tornando a própria imagem da humanidade. É onde estão agora os nossos autoícones.

A imagem vendida ao consumidor é comodidade, acessibilidade, valorização do tempo, ou seja, praticidade nas diligencias cotidianas junto aos bancos (*e-banking*), compras simplificadas em lojas online (*e-commerce*) e divagações e criação de diários virtuais abertos ao público (redes sociais ou social *networking*); além de outros mecanismos como e-Gov, indústria 4.0, geolocalização, internet das coisas, inteligências artificial, machinelearning, Big

Data e a computação ubíqua, todas com a consequência final de gerar uma fusão simbiótica entre seres humanos e máquinas.

Quanto a esses dois últimos mecanismos (Big Data e computação ubíqua), interessa-nos fazer alguns parênteses explicativos interessantes.

O termo Big Data começou a ser cunhado no início dos anos 2000, pelo professor Doug Laney, o qual o definiu nos clássicos 3 V's: *Data Volume*, *Data Velocity* e *Data Variety* (LANEY, 2012, *online*). Basicamente, o Big Data permite que certas atividades de tratamento de dados pessoais possam ser sintetizadas numa velocidade e variedade que possibilitam a substituição humana quase na totalidade, tanto em tempo, quanto qualidade no processamento, possibilitando o uso mais eficiente dessas informações no cenário econômico mundial.

Quanto as suas principais características, explicam González Allonca e Ruiz Martínez (2016, p. 1-2, *e-book*):

> Son características definitorias de la actividad del Big Data el tratar informaciónen grandes volúmenes, utilizando la totalidad de los datos disponibles (variedad), y a altas velocidades (indispensable, dada la magnitud de la información). Estas características del Big Data son conocidas como "lastres V": volumen, variedad y velocidad; para lo cual se requiere el desarrollo y la utilización tanto de hardware como de software específicos.
> [...]
> el Big Data permite obtener de ciertas actividades de tratamiento de datos personales - conexiones de equipos a redes (ej. telefonía), navegación em sitios o redes sociales en Internet, etc.- múltiples conclusiones sobre las conductas de los individuos, por ejemplo, señalar su proclividad a determinadas acciones, o establecer índices de probabilidad sobre estados y situacion es del sujeto (económicas, de salud, etc.), y determinar así la toma de decisiones por parte de los actores económicos del mercado. Debido a suvelocidad, el uso de Big Data ha ayudado a obtener, en un breve lapso de tiempo, conclusiones que por los médios tradicionales hubiera tomado meses, permitiendo ágilmente que el analista de datos pueda cambiar sus ideas basándose en el resultado obtenido y volver a procesarlos hasta encontrar el resultado esperado.

Já no que diz respeito à computação ubíqua, o seu objetivo, segundo Boff (2018, p. 133 e 137):

> [...] é integrar totalmente a relação tecnologia/máquina com os seres humanos, de forma que seja invisível, no sentido de automático (utilizar sem perceber). Os computadores passam a fazer parte da vida das pessoas de tal maneira que se tornam

> ‘humanos’, com seus sistemas inteligentes, que os tornam onipresentes.
> [...]
> Eis aqui o paradigma que norteia o desenvolvimento de um meio ambiente digital que congrega ubiquidade, pervasividade e inteligência, sendo o elemento de ligação formado pelo conjunto de dados veiculados, capturados, tratados e armazenados.

É certo que quando contemplado de forma científica, essa explosão de tecnologias de fácil acesso, com potenciais ainda desconhecidos, cria no indivíduo humano, inevitavelmente, uma meditação quanto a um cenário futuro verdadeiramente atemorizante. Boff (2018, p. 133), ao ter feito esse exercício de elucidação dos horizontes das novas tecnologias, apontou um exemplo que revela uma possibilidade de potencial lesividade, ou pelo menos instabilidade não revelada, nesse ambiente virtual:

> Pode-se adquirir um produto sentado em uma praça pública por meio de um site que não se sabe onde está hospedado, sendo que o produto comprado pode vir de uma terceira localidade ainda mais desconhecida.

Porém, outra premissa também deve ser dita: como essa instabilidade no sistema mundial não tem afetado o uso da tecnologia por parte das pessoas, mesmo naquelas que detêm o conhecimento desta realidade traçada na última citação, sobrou às empresas uma oportunidade de mercado super rentável, a qual lhes permitem alcançar determinado público alvo e ofertar-lhe bens e serviços numa nova plataforma de vendas moderna, sob a garantia de fluxo constante de consumidores, expandindo, assim, suas projeções econômicas para um futuro economicamente promissor.

Num devaneio de possibilidades que o futuro possa trazer, Harari (2018, p. 78-79) criou um cenário no qual o acesso aos dados pessoais das pessoas terá um impacto para além de tudo que se tem como realidade hoje:

> [...] no século XXI, os dados vão suplantar tanto a terra quanto a maquinaria como o ativo mais importante, e a política será o esforço por controlar o fluxo de dados. Se os dados se concentrarem em muito poucas mãos — o gênero humano se dividirá em espécies diferentes.
> [...]
> O que vai acontecer quando pudermos perguntar ao Google: “Oi, Google, com base em tudo o que você sabe sobre carros e com

> base em tudo o que você sabe sobre mim (inclusive minhas necessidades, meus hábitos, minhas opiniões sobre o aquecimento global, e até mesmo minhas ideias sobre a política no Oriente Médio), qual é o melhor carro para mim?". Se o Google for capaz de dar uma boa resposta, e se aprendermos com a experiência a confiar no bom senso do Google em vez deem nossos sentimentos facilmente manipuláveis, qual será a utilidade das propagandas de carro?

Embora pareça faltarem ainda algumas décadas para se chegar nesse nível de refino de dados ao ponto do ser humano se tornar totalmente dependente da máquina[12], o certo é que a posse plena desses dados significará um mapeamento completo do consumidor, como ideais políticos, religiosos, doenças, gostos. O Facebook e a Netflix têm ideias neste sentido, as quais, intencionalmente, ou não, geram a expectativa de aceleração dessa transição de controle de dados de humanos por máquinas (FOUQUET, GRANT, LI e MAWAD, 2018, *online*):

> [...] o Facebook está considerando oferecer uma versão de seus serviços sem propaganda para os clientes que estiverem dispostos a pagar. Não se trata apenas de refrear anúncios assustadores. A capacidade de processar grandes quantidades de dados pessoais promete mudar nossos relacionamentos, nossos governos e até mesmo nossos corpos - sem falar, é claro, de nossos hábitos de consumo.
> A Netflix já está usando dados de clientes para criar programas de TV e em breve os carros inteligentes poderão alertar as operadoras de rodovias sobre buracos na estrada ou acionar anúncios de outdoor diferentes para motoristas que estiverem escutando música country ou hip hop.

Para o bem, ou para o mal, é nesse cenário pitoresco que se encontra a humanidade, e por mais que a priori possa parecer algo ficcional, basta uma olhada rápida para a realidade para perceber que essas mudanças não estão adstritas somente às futuras gerações.

---

[12] Nina Hirata, se referindo a multiforma que a captação dos dados podem tomar, como a captação de dados por imagens publicadas (no Instagram, por exemplo, são publicadas 95 milhões de fotos todo dia) e até de vídeos publicados (no YouTube, são 300 horas de vídeos publicados por minuto), aponta que "Em captura de imagem estamos bem, mas ainda é preciso melhorar a análise dessas imagens por meio do aprendizado de máquina. A ideia é usar o computador para extrair qualquer tipo de informação útil e relevante a partir dos dados". Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/gigantes-da-tecnologia-ganham-bilhoes-com-uso-de-dados-de-pessoas-para-distribuir-anuncios-segmentados.ghtml>. Acesso em: 18 set. 2020.

Também é nesse cenário que se percebe de pronto que, sendo os dados o ouro do futuro, e guardando eles um potencial lesivo enorme à vida das pessoas, já que podem ser triangulados para se saber de alguém mais do que ele mesmo sabe, e ainda serem utilizados para fins escusos, não é de se estranhar o nascimento em nível mundial das regulamentações sobre o uso de dados pessoais[13].

É inegável que essas regulamentações têm o potencial de fomentar a economia mundial, haja vista o tratamento de dados sair dos bastidores e se mostrar agora com legalidade. Biondi e Monteiro (2019, p. 232) analisam essa fomentação[14]:

> Uma Lei Geral de Proteção de Dados Pessoais/LGPD tem por objetivo não só garantir a privacidade e outros direitos fundamentais dos cidadãos, mas, também, fomentar a economia. Ao mesmo tempo em que se reduz a assimetria de informação entre entidades privadas, públicas e indivíduos, franqueando aos últimos o controle sobre suas informações pessoais [...] estabelece-se alicerces claros para a utilização e monetização dessas informações. Com isso, garante-se, em última análise, segurança jurídica para tais relações. Ao invés de um custo operacional, os setores regulados, principalmente a iniciativa privada, podem e devem enxergar a proteção dos dados pessoais como um elemento de inovação e fomento à economia.

No entanto, o grande quesito que se apresenta, e que merece estudo e resposta, é: como as empresas estão se beneficiando dos dados de seus consumidores para gerarem riqueza? Como funciona a venda de dados no setor da saúde? De quanta riqueza se está falando?

---

[13] Essa necessidade de controle dos dados está sendo algo tão latente no mundo, que desde a entrada em vigor da GDPR, 117 países já promulgaram as suas respectivas regulamentações e 40 países estão ou em projeto de lei ou em trâmite de aprovação. (Dados colhidos em agosto de 2018 (DONEDA, Danilo. *A Lei Geral de Proteção de Dados Pessoais*. XXXVIII Congresso Internacional da Propriedade Intelectual da Associação Brasileira da Propriedade Intelectual – ABPI: agosto de 2018.)

[14] Foi nessa esteira que a *Asia-Pacific EconomicCooperation* (APEC) se propôs a criar o bloco de definições e princípios intitulados “Privacy Framework”, com intuito primordial de expandir o comércio eletrônico. Disponível em: <https://www.apec.org/search?Query=Privacy+Framework>. Último acesso em: 18 set. 2020; <https://www.apec.org/Press/News-Releases/2007/0122_aus_privacyprinciples>. Último acesso em: 15 jul, 2019; https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.aspx. Último acesso em: 18 set. 2020.

2.1 O mercado de dados pessoais sensíveis

Muito embora o capítulo dois desse trabalho traga maiores detalhes, acreditamos ser interessante fazer uma breve conceituação e enquadramento jurídico do que seriam os dados sensíveis para podermos estruturar as ideias seguintes com maior precisão.

Os dados sensíveis são uma espécie de dados pessoais (DONEDA, 2006, p. 160), distinguindo destes por seu conteúdo possuir uma carga maior de intimidade, gerando no titular de tais dados maior vulnerabilidade perante terceiros.

Nos termos formais do inciso II, do art. 5º, da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), compreende dados sensíveis:

> "[...] 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".

Ou seja, segundo Bioni (2019, p. 119), ao fazer a distinção entre generalidade e especificidade dos dados pessoais e sua correlação com os dados sensíveis:

> Ainda que, assim como um dado anônimo pode se tornar um dado pessoal, um dado "trivial" pode também se transmudar em um dado sensível; particularmente, quando se têm disponíveis tecnologias (e.g., Big Data) que permitem correlacionar uma série de dados para prever comportamentos e acontecimentos [...]. É possível, portanto, identificar individualidades mais sensíveis das pessoas, tais como orientação sexual, raça e estado de saúde, a partir de informações triviais.

Dada essas informações prévias, pode-se concluir com facilidade que os dados pessoais sensíveis de uma pessoa a atinge no mais íntimo do seu ser, e, por causa disso, possuem um potencial de mácula primária na honra e imagem da vítima nos casos possíveis de violação.

O mais curioso é que nos sistemas virtuais cotidianos, que exigem o preenchimento de formulários ainda que tão somente para gerarem um cadastro de consumo em determinada plataforma de compras online, a maioria desses

dados sensíveis já estão sendo fornecidos sem qualquer relutância pelo próprio consumidor.

É nessa esteira que, atualmente, um dos maiores nichos de mercado está atrelado justamente à posse e uso de dados pessoais de consumidores, geralmente fornecidos por eles mesmos, saibam ou não que estão fornecendo (DUHIGG, 2017, p. 195-225).

Isso chega a ser lógico, pois para manter a correlação de interdependência entre os proprietários das facilidades virtuais e seus consumidores, tentando manter uma relação de “intimidade” com quem nunca irá ver pessoalmente, é necessário conhecer mais um pouco das particularidades e comportamentos dos pretensos usuários dos produtos ou serviços.

Aqueles dados que as pessoas fornecem até no banheiro, não são dados perdidos. Ao contrário, eles são guardados em servidores que a partir daí podem ter diversos usos. Lippstein (2015, p. 6) alude quanto a estrutura de processamento desses tipos de dados:

> A inteligência dos dados em rede é tão bem organizada que os sistemas reúnem informações sobre os acessos, interesses, buscas de cada pessoa e traduzem isso em ofertas, e-mails, anúncios que compatibilizam com o histórico de assuntos pesquisados por determinado indivíduo, isso também é uma forma de demonstrar que os dados digitais estão desprotegidos uma vez que estão vulneráveis ao acesso ou conhecimento de suas informações para atender interesses de mercado e de publicidade.

Ou seja, esses dados são triangulados pelas empresas e servem tanto para mapear os consumidores para lhes venderem o que tem maior chance de ser comprado, como para melhorarem seus serviços. Veja-se um exemplo de como isso funciona[15]:

> 1.Ao criar um anúncio, em forma de post, é possível discriminar quais as características dos indivíduos a serem atingidos pelo conteúdo;
> 2.Esses usuários podem ser selecionados com base em detalhes banais (como idade e gênero), mais refinados (localização e renda) e até mais complexos (preferências políticas, culturais etc.);

[15] Exemplo dado pelo pesquisador do Laboratório de Estudos sobre Imagem e Cultura da Universidade Federal do Espírito Santo (LABIC/UFES) entrevistado pelo G1. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/gigantes-da-tecnologia-ganham-bilhoes-com-uso-de-dados-de-pessoas-para-distribuir-anuncios-segmentados.ghtml>. Acesso em: 18 set. 2020.

> 3.Esses interesses são traçados com base em informações que os próprios usuários cedem, em dados coletados pelas empresas sobre o comportamento deles na internet (e fora dela) e também nas conclusões tiradas pelas companhias após analisar tudo isso;
> 4.Os anunciantes não sabem quem são as pessoas a quem enviarão propaganda, apenas a que grupo pertencem.

Essa junção de inteligência artificial e tratamento de dados tem atingido sensibilidades que transpassam com facilidade as próprias informações que alguém tem de outrem num ambiente social e até privado. Um bom exemplo é o próprio Facebook, no qual, num estudo dirigido pela *Psychometrics Centre*, da *University of Cambridge*, com uma amostra de 58.466 voluntários dos Estados Unidos da América, utilizando o aplicativo *myPersonality* no próprio Facebook, se conseguiu, utilizando o método que será descrito a seguir, identificar com exatidão a porcentagem dos usuários homossexuais e heterossexuais, os usuários brancos e negros e, até, republicanos e democratas; ou seja, noutros termos, se descobriu que é possível traçar perfis de personalidade de um usuário com um refino possível maior do que alguém íntimo seria capaz de fazer (UNIVERSITY OF CAMBRIDGE, 2015, *online*):

> In the study, a computer could more accurately predict the subject's personality than a work colleague by analysing just ten Likes; more than a friend or a cohabitant (roommate) with 70, a family member (parent, sibling) with 150, and a spouse with 300 Likes.
> Given that an average Facebook user has about 227 Likes (and this number is growing steadily), the researchers say that this kind of AI has the potential to know us better than our closest companions.
> The latest results (...) which showed that a variety of psychological and demographic characteristics could be predicted with startling accuracy through Facebook Likes.

Porém, o mesmo experimento concluiu que um dos principais problemas desses cruzamentos de dados se dá pela falta de conhecimento das partes envolvidas sobre essas atividades. São consumidores que nem imaginam que terceiros já possuem informações não foram dadas por livre liberalidade do titular das informações à outrem, fazendo, no caso, com que aquele terceiro estranho se porte com maior intimidade perante a vítima do que mesmo seus amigos mais íntimos, como explicam Kosinski, Stillwell e Graepel (2013, *online*), ao comentarem a referida pesquisa:

> On the other hand, the predictability of individual attributes from digital records of behavior may have considerable negative implications, because it can easily be applied to large numbers of people without obtaining their individual consent and without them noticing. Commercial companies, governmental institutions, or even one's Facebook friends could use software to infer attributes such as intelligence, sexual orientation, or political views that an individual may not have intended to share. One can imagine situations in which such predictions, even if incorrect, could pose a threat to an individual's well-being, freedom, or even life. Importantly, given the ever-increasing amount of digital traces people leave behind, it becomes difficult for individuals to control which of their attributes are being revealed. For example, merely avoiding explicitly homosexual content may be insufficient to prevent others from discovering one's sexual orientation.

No outro lado da esteira, essa realidade não vem só com intenções de triangulação de dados para melhoramento de serviços ou maior comodidade do consumidor. Junto às novas possibilidades de usos de dados para melhorar a vida das pessoas, nascem, também, novas modalidades de comércio ilegal de dados, tão refinado quanto às práticas ilícitas no plano físico, com suas próprias nomenclaturas e *modus operandis*¸ como se vê claramente na investigação independente do site TecMundo (2015, *online*):

> O submundo do comércio ilegal de dados parece ter criado uma linguagem própria para facilitar a comunicação entre seus membros, assim como membros de quadrilhas utilizam códigos e símbolos variados para se identificar entre outros participantes de sua própria tribo. Um especialista em venda de cartões de crédito (os chamados "CCs"), por exemplo, é chamado de *carder*, enquanto um hacker focado em fraudes bancárias identifica-se como um *banker*. Já as contas-laranja usadas para firmar negociações são conhecidas como *laras*.
> Por R$ 600, poderíamos comprar uma credencial para o database do Departamento Nacional de Trânsito (Denatran). Mais um período de testes e mais uma surpresa: Fênix também utiliza o sistema Rei das Consultas, o mesmo empregado pelo Moc Consultas. Posteriormente, descobrimos que Fênix é, na verdade, o fornecedor do tal painel. Ao realizar login na central, porém, apenas os databases do Detran e do CADSUS estavam ativos. Testamos o primeiro e, informando apenas o CPF da vítima, obtivemos acesso a todos os dados de seu veículo.

Em 2018, o poder econômico (e lesivo) do uso de dados de terceiros recebeu uma prova mais contundente do potencial lesivo do mau uso dos dados pessoais dos consumidores no caso envolvendo a empresa americana Cambridge Analytica e o Facebook.

Contextualizando o ocorrido, é precisa sabe que embora haja uma variedade grande de redes sociais que surgiram depois do Facebook, esta ainda continua sendo uma das *socials networking* mais utilizadas no mundo (CUSTÓDIO, 2018, *online*). O fluxo de pessoas nos seus servidores, sob o marketing do “livro de rosto” para que todos pudessem acompanhar as vidas uns dos outros, mostrou-se valioso para que o próprio Facebook “disponibilizasse” os dados deixados por cerca de 87 milhões de seus usuários para a Cambridge Analytica, para que esta fizesse propaganda política prol Trump (MIGUEL, 2019, *online*), incluindo, inclusive, dados referentes aos amigos daqueles usuários violados (G1, 2018, *online*).

O resultado dessa operação é que o Facebook terá que pagar a multa recorde de 5 bilhões de dólares para encerrar as investigações sobre o vazamento dos dados (REUTERS, 2019, *online*), sem falar na perda de 128 bilhões de dólares em valor de mercado após a divulgação dos vazamentos (CAPELAS, 2018, *online*), e ainda ficar com a tarja de ter contribuído verdadeiramente na eleição presidencial dos Estados Unidos da América.

Em 2016, uma grande polêmica também mexeu com a Austrália. A prestadora de serviços de coleta e doação de sangue, a *Red Cross Blood Service,* apresentou problemas de segurança no tratamento de dados dos doadores de sangue, ocasionando o acesso de cerca de 550.000 doadores por pessoas não autorizadas, entre 2010 e 2016. Se isso por si só já é suficiente para provar o potencial de dano em não fazer adequadamente o tratamento de dados sensíveis de terceiros, a lesão se agravou quando descobriram que os acessos permitiam ver os cadastros/relatórios dos pacientes, os quais revelavam um dado, em especial, muito constrangedor: se o doador tinha praticado algum comportamento sexual de risco nos últimos 12 meses (ABC NEWS, 2016, *online*).

Em 2017, foi a vez de uma empresa canadense mostrar a necessidade de um controle sobre o uso de dados não autorizados por terceiros. A *Standard Innovation*, especializada em criar itens para práticas sexuais, criou um moderno vibrador que se conectava por rede a um celular, por meio de um aplicativo. O problema é que não foi contado aos consumidores que o aparelho enviava para os servidores da empresa as informações de uso do produto, como tempo de uso, quais vibrações mais estavam sendo usadas por aquele cliente, e, até, a

temperatura corporal do consumidor durante o uso do produto (HERN, 2017, *online*).

No Brasil, um caso polêmico envolveu a Anatel. Quando esta anunciou que compraria quase 1 bilhão de reais de equipamentos com potencial de extrair dados confidenciais dos seus consumidores, como registros de chamadas feitas e recebidas, o tempo de duração das ligações e data e horário delas, houve um grande incômodo tanto nos consumidores, quanto em juristas que questionavam a legalidade de tal ato (VELOSO, *online*). Para que serviriam esses dados? Somente para melhoramento do sistema?

Outra polêmica envolveu o Serasa Experian e Serviço Central de Proteção ao Crédito. Só o Serasa tem acesso a dados de mais de 170 milhões de consumidores, como nome completo, números de documentos, INSS, endereço, telefones, idade, data de nascimento, sexo, estado civil, escolaridade, padrões de consumo, profissão, renda familiar, dados do cônjuge, nome da mãe, participação societária em empresas, participação em empresas falidas, ações judiciais, referências bancárias (número da conta e agência), status na Receita Federal, informações de cheques, ações na Justiça, score de crédito (pontuação que indica a possibilidade do consumidor pagar ou não a dívida), falência de empresas, entre outros, e tudo sem nem ao menos o consumidor saber ou concordar com a posse desses dados sensíveis e muito menos autorizar sua venda, como vem sendo feito (SILVA, *online*).

No entanto, uma das investigações mais interessantes já realizadas quanto ao valor de mercado dos dados sensíveis foi feita pelo repórter Pablo Fernandez. Buscando descobrir o quanto seria difícil obter acesso a dados de consumidores avulsos, o repórter da BandNews FM durante quatro meses investigou um grande esquema de venda de dados pessoais extraídos, inclusive do INSS, Forças Armadas e serviço federal (nem o Presidente da República e o Ministro da Justiça estavam protegidos), como números de telefones (celulares ou fixos), números de documentos pessoais, endereços, dados bancários, salários e informações de parentes. O fim de tais dados era o mercado de *call center* (BANDNEWSFM, *online*). Conforme se extrai dos resultados obtidos pelo repórter investigativo:

> Tudo isso é negociado diariamente por sites, que são utilizados, na maioria das vezes, por empresas de telemarketing em todo o Brasil. Pelo Hotfone, nome dado aos sistemas que permitem a consulta de dados pessoais, é possível encontrar qualquer pessoa. Qualquer um mesmo! Pode ser ministro, governador, presidente ou você.
> Parte das páginas, no entanto, sequer aparece nas buscas do Google, para não levantar suspeita. Por meio de grupos no Whastapp, a BandNews FM identificou pelo menos oito sistemas – a maioria com informações colhidas em servidores utilizados pelo INSS, Forças Armadas ou do serviço federal; alguns têm um banco de dados próprio e não está claro como são abastecidos.
> O preço varia conforme o tipo de pacote: há sites com planos mensais, que podem custar entre 75 e 100 reais, e há ainda a possibilidade de comprar um número fechado de consultas, como mostra a negociação feita com uma mulher que comercializa acessos ao site Consulta Mais: "Eu tenho quantidade de 1.000 consultas, 5.000 ou 10.000. Você compra 1.000 consultas, eu vou te depositar 1.000 consultas no seu usuário e você vai usar as 1.000 consultas até elas esgotarem. 1.000 consultas ficam 300 reais".

Como se vê, em nada muda a uma verdadeira feira online de venda de dados, sendo o trabalho do comprador tão somente fazer o refino necessário aos seus gostos e ter acesso a uma infinidade de informações, as quais, literalmente, tem o poder de mudar completamente a vida de uma pessoa para pior.

Uma importante pesquisa encomendada pela CA Technologies, e realizada pela renomada empresa Frost&Sullivan, intitulada "*Global State of Digital Trust Surveyand Index 2018*", extraiu os locais de trânsito dos dados pessoais nas suas próprias organizações, e, ainda, analisou as opiniões de consumidores, profissionais de cibersegurança e executivos sobre confiança digital.

Como se extrai do relatório final gerado na pesquisa, as suas organizações violavam as informações pessoalmente identificáveis (*Personally Identifying Information*, PII, como sigla em inglês) e 43% dos líderes de negócios também vendiam tais dados (FROST & SULLIVAN, 2018, p. 11).

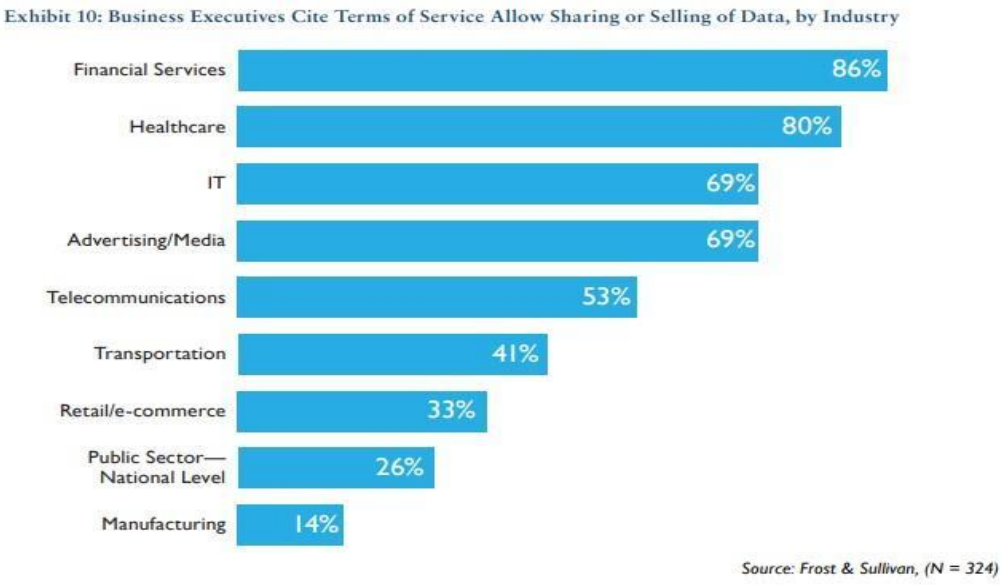
O relatório continua afirmando que apenas 15% dos profissionais de cibersegurança pesquisados eram cientes da venda de dados PPI (*idem*, p. 13), ou seja, criou-se uma estrutura na qual os dados são vendidos de forma a não democratizar a informação com todos os profissionais envolvidos, possuindo somente uma pequena cúpula na manutenção dos controles de danos e aperfeiçoamento.

Não é sem motivo que 78% dos consumidores responderam que é muito importante ou crucial terem seus dados sensíveis online protegidos e 48% dos consumidores relataram abandonar os serviços de uma organização envolvida em uma violação de dados (*Idem*, p. 3), gerando, com isso, um sentimento ambivalente: por um lado os consumidores fornecem todos os dados que um simples cadastro exige, sem questioná-los, mas acreditando que estarão protegidos em servidores, em contrapartida, tomando conhecimento que esses mesmos dados não estão somente num sistema, mas sim sob acesso direto de pessoas físicas que os usam de formas das mais variadas, cria-se uma aversão a tal prática, chegando mesmo a condená-la.

O resultado da pesquisa foi que o Índice de Confiança Digital global é de 61 pontos, de um total de 100 (*Idem*, p. 4).

De fato, todas essas informações extraídas, tanto da Cambridge Analytica, Anatel, Serasa Experian e Serviço Central de Proteção ao Crédito, a investigação de Pablo Fernandez e o relatório encomendado pela CA Technologies, revelam que existe um mercado - às vezes negro - de venda de dados cujo valor chega a ser incalculável, revelando, ainda, que a venda de dados pessoais tem se tornado uma prática comum e vem se alastrando em nível mundial.

No entanto, um fato bastante curioso salta aos olhos quando analisado um gráfico do relatório da CA Technologies. Fazendo um levantamento detalhado dos setores para os quais uma das organizações da *CA Technologies* mais vendiam os dados pessoais dos seus clientes, tem-se a seguinte lista (*idem*, p. 11):



Como se vê no gráfico acima, o setor da saúde é o segundo maior destino da venda de dados. Os motivos não foram deixados claro, mas o que se sabe sobre esse setor é que só a indústria farmacêutica chegou a movimentar, no Brasil, em 2018, quase R$ 120 bilhões, correspondendo a um crescimento de 11,89% em comparação ao ano antecedente (IPDFARMA, 2019, *online*), e chegando a ter uma projeção de crescimento até 2023 para R$ 175 bilhões (PINHEIRO, 2019, *online*), e, unindo os pontos, ter conhecimento antecipado das demandas farmacológicas de consumidores e ofertá-las explorando ao máximo todo seu potencial econômico é, sem dúvida, algo extremamente lucrativo, e potencialmente abusivo, ao mesmo tempo.

Colocando isso em perspectiva, para manter essa alta lucratividade do setor da saúde, o qual dispõe da posse de dados sensíveis de pacientes para usos que não são deixados claros, tem-se mantido um sistema de desvantagem para com os pacientes, os quais podem estar sendo vítimas dos seus próprios infortúnios, já que os dados estão sendo colhidos nos momentos das suas entradas em hospitais, clínicas e farmácias, estas aproveitando a oportunidade para extrair dados sensíveis sem que nem ao menos os pacientes saibam que estão sendo extraídos, muito menos autorizando suas extrações.

Exemplo disso é a atividade explícita da empresa IMS Health, a qual abriu seu capital em 2014, e tem como seu objeto social a compra e venda de informações sobre a saúde dos pacientes, não fazendo questão de esconder que a empresa detém informações de 85% de todas as receitas médicas prescritas no mundo, chegando, com isso, a deter o monopólio do mercado (CARVALHO, 2014, *online*). Basicamente, esse é seu *modus operandis*:

> [...] toda vez que você passa por um pronto socorro, faz algum exame ou compra algum remédio, está fornecendo dados para um hospital, laboratório ou farmácia.
> Sexo, idade, sintomas, quais remédios vai tomar e quem foi o médico que o atendeu são alguns desses dados. Essas informações são vendidas para empresas, que as compilam, analisam e revendem para gigantes farmacêuticas.
> Com esses dados é possível prever, por exemplo, quais as chances de sucesso de determinado medicamento no mercado, qual o preço aceitável e quais são os produtos que terão maior demanda em um futuro próximo. É possível, também, saber os perfis dos médicos e o que eles costumam prescrever, o que facilita as ações de marketing por parte das empresas.

Outra forma de como esses dados ganham valor de mercado foi descoberta pelo Ministério Público do Distrito Federal, ao deflagrar uma investigação, em 2018, por meio da Comissão de Dados Pessoais da própria instituição, contra farmácias que apresentavam indícios de venda de dados pessoais sensíveis. Segundo o coordenador da investigação, o promotor Frederico Meinberg (LUIZ, 2018, *online*):

> Existe uma verdadeira obsessão das farmácias em dar desconto. E no capitalismo, não existe obsessão de graça. Há um interesse por trás. Imagine que você comprou no seu CPF um remédio para sua avó que está sofrendo de câncer. Se esse histórico sai da farmácia e é compartilhado com outros setores, numa análise, o plano de saúde pode acreditar que você está fazendo um tratamento e não avisou. Daí aumentam o valor do contrato e você nem fica sabendo. Vamos pegar um hipocondríaco, que compra remédio todo dia, e um outro homem que tem a mesma idade, mas morre de medo do médico. O primeiro pode vir a pagar um plano de saúde muito mais caro do que o outro. É importante entender que seus dados fazem parte do seu patrimônio. O brasileiro tem uma coisa muito perigosa: diz que não tem nada a esconder. Mas essas informações sigilosas têm um valor enorme.

Nessa esteira, se vê que o uso de dados de forma indiscriminada, e irresponsável, tem um impacto econômico digno de atenção, tanto para o bem (riqueza), quanto para o mal (prejuízo financeiro, social e moral).

Quando se fala de consumidores, não há como deixar de lado a sua hipossuficiência presumida, a qual busca balizar as relações de consumo de modo a priorizar a parte mais frágil na relação de consumo.

Em contrapartida, não há, também, como não acender um alerta às empresas do setor de saúde, principalmente, as quais precisam tratar os dados pessoais sensíveis dos seus pacientes, para que se atentem as novas diretrizes trazidas pela nova Lei Geral de Proteção de Dados Pessoais brasileira para o tratamento desse tipo de dados. Ao invés de vê-la como um empecilho, é importante que as empresas a enxerguem como uma ferramenta moderna de tendência mundial que somará no aperfeiçoamento da lida diária dos referidos dados de forma a resguardar tanto o consumidor/paciente, mas também a empresa.

2.2 A potencial lesividade aos direitos fundamentais

Quando se fala em proteção aos dados pessoais (sensíveis ou não), se está falando diretamente à dignidade da pessoa humana. Não é sem motivo que, embora escrito na maioria em termos gerais, a Declaração Universal dos Direitos Humanos, desde o seu nascimento em 1948, já fazia alusão aos cuidados morais e legais que se deveria ter com o ser humano, quanto pessoa, como bem alude os artigos VI e XII da referida Declaração:

> Artigo VI Todo ser humano tem o direito de ser, em todos os lugares, reconhecido como pessoa perante a lei.
> Artigo XII Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.

Buscando elucidar de forma doutrinária e trazendo as diferentes concepções que o termo dignidade da espécie humana pode ter conforme a sensibilidade hermenêutica, Sarmento (2016, p. 27-28), trazendo um conceito, afirma que:

> A dignidade da espécie humana consiste no reconhecimento de que o ser humano ocupa uma posição superior e privilegiada entre todos os seres que habitam o nosso mundo. Distintas razões foram empregadas para justificar essa superioridade, sendo as mais frequentes o uso da razão, o livre arbítrio e, no âmbito religioso, a criação à imagem de Deus. Já a dignidade da pessoa humana envolve a concepção de que todas as pessoas, pela sua simples humanidade, têm intrínseca dignidade, devendo ser tratadas com o mesmo respeito e consideração.

O princípio da dignidade da pessoa humana, sem dúvida, é um importante fundamento da ordem jurídica e da comunidade política (SARMENTO, 2016, p. 77). Quando se passa a olhar o ser humano como uno, sem distinção de raça, sexo, credo, condições sociais e financeiras, não o vendo mais como objeto de subjugo, tão presente na história de dominação de uma nação/povo sobre outros, então se encontrará tal princípio concretizado em todas as sendas do ideal social da liberdade, igualdade e solidariedade.

Nessa esteira, ao complementar a premissa acima, tratando do princípio da dignidade da pessoa humana se aplicando na situação jurídica existencial, acertadas são as palavras de Mulholland (2018, p. 170 *e-book*):

> A análise do princípio da dignidade da pessoa humana se realiza, portanto, e com razão, considerando-se sempre a plena tutela da pessoa, seja considerando aspectos relacionados à sua liberdade, seja à sua identidade e privacidade, como no caso dos dados pessoais.

Numa leitura mais detalhada, é possível encontrar duas acepções para o princípio em tela: uma no sentido mais material, no sentido de garantir a todas as pessoas humanas um tratamento digno de sua natureza, sem tortura ou tratamento degradante, sem ofensa a sua integridade física e psicológica; e outra, num sentido mais abstrato, buscando criar mecanismos, com propostas e projetos, que viabilizem a concretização do tratamento digno a todas as pessoas humanas. (MULHOLLAND, 2018, p. 169, *e-book*).

No Brasil, quando os Direitos Fundamentais positivaram alguns dos principais direitos humanos, principalmente na Constituição da República Federativa do Brasil, de 1988, se ganhou, logicamente, uma proteção garantista mais personificada. Esses Direitos Fundamentais, formam um aglomerado intricado e diversidade de várias análises jurídicas distintas (MARINONI, MITIDIERO e SARLET, 2018, *e-book*).

Buscando conceituar esses direitos, que já foram exaustivamente estudados e redimensionados na doutrina e jurisprudência pátria, Araújo (2005, p. 109-110) parece acertar ao afirmar que:

> Os direitos fundamentais podem ser conceituados como a categoria jurídica instituída com a finalidade de proteger a dignidade humana em todas as dimensões. Por isso, tal qual o ser humano, tem natureza polifacética, buscando resguardar o homem na sua liberdade (direitos individuais), nas suas necessidades (direitos sociais, econômicos e culturais) e na sua preservação (direitos relacionados à fraternidade e à solidariedade).

Num desses redimensionamentos, o tema relativo à universalidade dos direitos fundamentais ganhou nova leitura. Basicamente, a universalidade se relacionava, originalmente, como a forma com a qual o ser humano era visto quanto pessoa, tendo como pano de fundo a liberdade. Fazendo um aporte a essa nova universalidade dos direitos fundamentais, Bonavides alude (2004, P. 573):

> Os direitos da primeira, da segunda e da terceira gerações abriram caminho ao advento de uma nova concepção de universalidade dos

> direitos humanos fundamentais, totalmente distintas do sentido abstrato e metafísico de que se impregnou a Declaração dos Direitos do Homem de 1789 [...] A nova universalidade dos direitos fundamentais os coloca assim, desde o princípio, num grau mais alto de juridicidade, concretude, positividade e eficácia. [...] não exclui os direitos da liberdade, mas primeiro os fortalece com as expectativas e os pressupostos de melhor concretizá-los mediante a efetiva adoção dos direitos da igualdade e da fraternidade. [...] A nova universalidade procura, enfim, subjetivar de forma concreta e positiva os direitos da tríplice geração na titularidade de um indivíduo que [...] é pela sua condição de pessoa um ente qualificado por sua pertinência ao gênero humano, objeto daquela universalidade.

Necessário se faz, também, não enxergar os direitos fundamentais como uma terra sem lei, sem limites, sem parâmetros de razoabilidade e proporcionalidade. Ao contrário, tais direitos são cheios de exceções, que se firmam como mecanismos de liquidez da realidade humana, os quais impedem que qualquer texto criado, por maior zelo que se tenha, possa alcançar todas as nuances que as relações humanas possam criar no dia a dia. Não é raro dois princípios fundamentais colidirem, de modo que a solução não poderá ser a anulação de um direito em detrimento do outro, mas a tentativa primária de harmonização; somente não sendo possível tal simbiose é que uma cláusula de exceção buscará, segundo a Lei de Introdução às Normas do Direito Brasileiro (Decreto-Lei nº 4.657/42), excluir um deles com base em critérios hierárquicos, cronológicos[16] ou da especialidade[17].

Com isso, ao fazer a análise do ser humano sendo considerado em si, estando essa premissa munida da robustez e proteção em nível constitucional, há de se considerar, logicamente, que toda a investida legislativa tem que ter como fim enxergar o homem e seus respectivos valores como o bem supremo. Porém, se por um lado não se pode enxergar tais direitos como absolutos, por outro, haverá uma limitação à interpretação do conteúdo desse axioma constitucional. Tratando disso, Mulholland afirma (2018, p. 169-170, *e-book*):

---

[16] Art. 2º [...] § 1º A lei posterior revoga a anterior quando expressamente o declare, quando seja com ela incompatível ou quando regule inteiramente a matéria de que tratava a lei anterior.

[17] Art. 2º [...] § 2º A lei nova, que estabeleça disposições gerais ou especiais a par das já existentes, não revoga nem modifica a lei anterior.

> Se for possível dizer que a dignidade da pessoa humana, por se erigir como fundamento do Estado Democrático de Direito, deve alcançar todas as esferas do ordenamento jurídico – incluído aí os institutos de Direito Privado –, é também possível concluir que a limitação interpretativa do conteúdo deste valor constitucional será difícil de se alcançar. Nesta dificuldade se encontram as barreiras para a aplicação consciente do princípio da dignidade humana.

Tal dificuldade se daria pelo risco à generalização, como se todos os direitos fundamentais pudessem sofrer modulações das mais variadas. Segundo Moraes (2003, p. 83) "[...] levada ao extremo, essa postura hermenêutica acaba por atribuir ao princípio um grau de abstração tão intenso que torna impossível sua aplicação."

Canalizando todas essas informações à proteção aos dados pessoais, se tem dois pontos de partida bem interessantes: 1) não há qualquer menção direta na Constituição Federal de 1988 à proteção de dados pessoais; 2) embora não exista menção direta, há uma forte base geral na própria Constituição, a qual servirá de referência para legislações futuras.

Segundo a Carta Maior (BRASIL, *online*):

> Art. 1º A República Federativa do Brasil[...] tem como fundamentos:
> [...]
> III - a dignidade da pessoa humana;
> [...]
> 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:
> [...]
> 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 [...]
> [...]
> LXXII - conceder-se-á *habeas data:*
> a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
> b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;

É possível perceber que mesmo na ausência de um texto legal explícito na Constituição Federal sobre o direito aos dados pessoais ser um direito fundamental, de forma alguma se pode afirmar haver uma omissão legal à proteção do referido direito.

Se afunilado com os princípios e valores da dignidade da pessoa humana que fora positivado na própria constituição, se terá o direito à privacidade como aquele que mais salta aos olhos da proteção dos dados pessoais. Por isso, acreditamos ser acertada a conclusão apresentada por Mulholland (2018, p. 171, *e-book*) de que: [...] os dados são elemento constituinte da identidade da pessoa [...] que devem ser protegidos na medida em que compõem parte fundamental de sua personalidade [...] por meio do reconhecimento de sua dignidade.

Nesse diapasão, necessário seria interpretar o alcance da Constituição, de modo: [...] a se extrair uma garantia geral de proteção da informação pessoal, que complementaria o atual sistema de garantias específicas de sigilo e da intimidade e da vida privada. (MENDES, 2014, p. 165).

No que diz respeito à Lei Geral de Proteção de Dados, que será tratada de forma mais técnica no próximo capítulo, seu intuito mais expressivo é justamente resguardar os direitos ligados à liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural (PINHEIRO, 2018, p.17), princípios estes extraídos da interpretação sistemática da própria Constituição Federal, como alude Mendes (2014, p. 168):

> Assim, entendemos que é possível, a partir de uma interpretação sistemática da Constituição, fundamentar uma garantia geral de proteção de dados pessoais no sistema de direitos fundamentais: partindo do reconhecimento da proteção da informação pessoal pela ação de habeas data e do princípio fundamental da dignidade humana, é possível ampliar a garantia da inviolabilidade da intimidade e da vida privada para a proteção de dados pessoais. [...] A finalidade do tratamento de dados pessoais mesmo que não estejam dispostos na Constituição Federal, podemos tratá-lo como direito protegido na mesma categoria do direito à inviolabilidade da intimidade e da vida privada [...] Ainda, através de uma interpretação de forma sistemática, podemos embasar a proteção constitucional com o princípio da dignidade humana e à luz da garantia constitucional do habeas data.

Esses dispositivos constitucionais estão revestidos pelas chamadas cláusulas pétreas, as quais lhes protegem de eventuais tentativas de

sucumbências tirânicas de qualquer dos três poderes federais. Tais cláusulas são (NEVES, 2014, p. 7, *online*):

> [...] formulações jurídicas destinadas a evitar a destruição ou a radical alteração da ordem constitucional. Constituem, pois, normas de controle, que permitem aferir a compatibilidade da revisão constitucional. Busca-se evitar o desmantelamento da ordem constitucional, bem como preservar a credibilidade histórica da *Lex Magna* do aviltamento de uma reforma excessiva. (Grifo original).

Em contrapartida, não é possível afirmar que a positivação explícita de um texto legal sobre a proteção aos dados pessoais das pessoas só foi inaugurada legalmente com o Regulamento Geral sobre a Proteção de Dados, criado pela União Europeia, ou com a Lei Geral de Proteção de Dados, aqui no Brasil.

No ano 2000, duas manifestações legais surgiram como sendo as pioneiras ao que seria uma regra num futuro de dezenove anos depois. Primeiro, a Carta dos Direitos Fundamentais da União Europeia, cuja intenção era criar um laço mais estreito de valores comuns entre os povos europeus, estabeleceu em seu artigo 8º o seguinte texto (CNPD, 2000, *online*):

> Artigo 8 – Proteção de dados pessoais 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

A segunda manifestação pioneira seria na Argentina. Após vir desenhando uma série de legislações pertinentes ao assunto (*Ley de Correos* 20.216, *La ley* 27.078 *de Tecnologías de la Comunicación y la Información*, *La ley* 26.529 *de Derechos de los Pacientes*, a lei 26.95112, por a qual se criou o *“Registro Nacional ‘No Llame’”*), finalmente, se criou, em outubro, a lei nº 25.326 de *“Protección de los Datos Personales”* (FERREYRA, 2017, *online*), basicamente com a mesma estrutura e alcance que seria visto nas legislações da União Europeia e do próprio Brasil.

No Brasil, o Marco Civil da Internet (Lei n° 12.965/2014), no seu art. 2º, inciso II, deixou claro que a preocupação que se deveria ter quanto ao uso da internet guardaria relação direta e necessária com (BRASIL, *online*): [...] os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais.

Em 2018, em conjunto ao Ministério da Ciência, Tecnologia, Inovações e Comunicações, além de outros apoiadores, e sob requerimento do Conselho de Desenvolvimento Econômico e Social, o Governo Federal lançou o documento intitulado “E-Digital – Estratégia brasileira para a transformação digital”, com intuito de propor uma agenda para a sociedade digital do futuro.

Na ocasião, acreditou-se que deveria se ter as garantias de direitos humanos também no ambiente digital, de modo a fazer nascer uma maior confiança por parte das empresas e indivíduos para com as regulações brasileiras no ambiente digital, dirimindo, com isso, qualquer tarja de ambiente digital hostil em território brasileiro. Nas conclusões do próprio trabalho (MCTIC, 2018, *online*):

> A garantia de direitos no ambiente digital é a pedra fundamental da confiança no ambiente digital. Não basta que empresas e indivíduos se sintam protegidos em relação a ataques cibernéticos e incidentes de segurança; é preciso que enxerguem o ambiente digital como um espaço em que o exercício de direitos está plenamente assegurado. Assim sendo, deve-se direcionar as novas tecnologias para a proteção de direitos e ao interesse público.
> [...]
> A primeira e mais fundamental é a dimensão dos direitos humanos. Liberdades de expressão, comunicação, manifestação, associação e direitos de acesso à informação e não discriminação precisam ser incorporados na arquitetura e governança da Internet. Violações dessas liberdades e direitos pelo Estado, empresas e mesmo por usuários precisam ser monitoradas e repelidas com vigor.
> [...]
> Garantir o direito à privacidade e à proteção de dados pessoais é um tópico particularmente relevante para o Brasil, dada a massiva adesão de brasileiros a redes sociais, aplicativos de mensagens instantâneas, internet banking e plataformas de comércio eletrônico.

Na ocasião de uma entrevista sobre aquela pesquisa *Global State of Digital Trust Surveyand Index 2018*, já exposta no item anterior, o Diretor de Cibersegurança para América Latina na *CA Technologies*, Julio Carvalho afirmou

ter percebido o recado dado pelos próprios consumidores (CRYPTOID, 2018, *online*):

> [...] os usuários estão mais exigentes em relação à proteção de suas informações pessoais e confidenciais e querem se associar a produtos e serviços alinhados com seus valores. [...] A confiança é passageira se as organizações não adotarem o processo para evitar que os dados dos consumidores caiam em mãos erradas. O sucesso na economia digital exige a adoção de uma mentalidade de segurança em primeiro lugar e a perda de confiança digital impacta diretamente todos os aspectos de um negócio e na percepção da marca.

Na mesma ocasião, Jarad Carleton, Diretor de Cibersegurança da Frost&Sullivan, empresa responsável pela pesquisa apontada, concluiu um interessante raciocínio (*idem*):

> O que a pesquisa constatou é que certamente existe um preço a pagar quando se trata de manter a privacidade das pessoas, não importa se você é um consumidor ou gerente de uma empresa que lida com dados de clientes. O respeito pela privacidade do consumidor deve ser um pilar ético para qualquer companhia que coleta dados de usuários.

Como já destacado, o artigo 5º, inciso X, da Constituição Federal, protege a intimidade, a vida privada, a honra e a imagem das pessoas. Talvez esse inciso seja o cerne dos cuidados com a proteção de dados pessoais. Embora seja um princípio genérico, abrangente para os diferentes fatos do dia a dia, sua positivação possibilita aplicá-lo a algo tão atual como é a proteção de dados pessoais, o alicerçando como um verdadeiro norteador à legislação nacional.

O próprio artigo 2º, da Lei Geral de Proteção de Dados Pessoais, elenca uma série de valores que acabam sendo verdadeiros princípios constitucionais, como: à privacidade; à autodeterminação informativa; à liberdade de expressão, de informação, de comunicação e de opinião; à inviolabilidade da intimidade, da honra e da imagem; ao desenvolvimento econômico e tecnológico e a inovação; à livre iniciativa, livre concorrência e defesa do consumidor e aos direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Porém, mesmo sendo aparentemente fácil fazer essa correlação entre o inciso X e a proteção a nível constitucional dos dados pessoais conforme o art. 2º, da LGPD, um grupo de senadores foi além, propôs um Projeto de Emenda à Constituição (nº 17, de 2019), o qual tramita hoje na Câmara dos Deputados, com intuito de acrescentar no art. 5º, o inciso XII-A, e no art. 22, o inciso XXX, com os seguintes textos: “XII- A - é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais; XXX- proteção e tratamento de dados pessoais.”. Como justificativa para tal criação, foi alegado que (BRASIL, 2019, p. 5):

> (...) o Brasil necessita muita mais do que uma lei ordinária sobre o assunto, apesar da envergadura jurídica da Lei no 13.709, de 14 de agosto de 2018 (LGPD), propomos a presente mudança à Constituição Federal.
> Nesta Proposta, também buscamos, além de instituir o direito fundamental à proteção de dados pessoais, também disciplinar questão tormentosa: a competência constitucional para legislar sobre o tema.

É possível que em algum momento excepcional, ante as multifacetas do cotidiano social, possa surgir uma celeuma que cobre dos aplicadores do Direito uma direção mais voltada à literalidade da Constituição Federal. Nesses casos, textos legais claros e límpidos, como os apresentas acima, serão uma fonte segura de condução à resolução dos possíveis impasses.

Essa PEC prova que os direitos fundamentais realmente não se esgotam; são, na verdade, uma construção histórica constante, nascendo conforme a sociedade evolui e ganhando novos desdobramentos sempre que necessário a evolução do trato social.

A melhor saída, no momento, para vestir a proteção dos dados pessoais de cláusula pétrea, seria considerá-la como um direito fundamental implícito, ainda que exija do hermeneuta fazer uma fazer interpretação extensiva em favor desse direito. Olhando desta perspectiva, interessante são as palavras de Rodotà (2018, p. 14), se está diante de uma verdadeira:

> [...] reinvenção da proteção de dados – não somente porque ela é expressamente considerada como um direito fundamental autônomo [...] mas também porque se tornou uma ferramenta essencial para o livre desenvolvimento da personalidade. A

> proteção de dados pode ser vista como a soma de um conjunto de direitos que configuram a cidadania do novo milênio.

Embora possam parecer medidas exageradas em algum momento, se analisado noutra perspectiva, agora de um ponto de vista onde os dados pessoais são meros direitos, e não direitos fundamentais, se perceberá, de pronto, que o tratamento de dados pessoais feito de modo irresponsável chega a ter maior potencial de danos ao homem médio do que "[...] os perigos 'tradicionais', que ensejaram o nascimento desse direito, como a hipótese de ser flagrado por paparazzi ou de ser notícia de jornais sensacionalistas." (MENDES, 2014, p. 171).

Isso posto, nos dias atuais não seria possível fazer uma leitura proporcional sobre tratamento de dados pessoais sem inclui-los no status de proteção fundamental à pessoa humana.

Os dados pessoais e a tecnologia fazem partes indissolúveis da vida dos consumidores, chegando a ser atualmente um reduto digital mais utilizado até mesmo do que os documentos físicos. Junto a isso, galgam incertezas provenientes do colonialismo digital que essa geração pioneira está tendo que enfrentar.

Nem sempre a tecnologia se mostrará ao lado do consumidor, de modo que reconhecer os dados daqueles que fornecem a nova riqueza do século XXI como "sagrados" é um importante passo para a evolução digital, jurídica e social.

4 O TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS, SEGUNDO A LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA

A humanidade está vivendo um fenômeno de transformação chamado por alguns de “Quarta Revolução Industrial”, no qual se tem visto a disponibilização à sociedade de novos instrumentos virtuais como a Digitalização, Internet das Coisas, Blockchain, Big Data, impressão 3D, engenharia genética, inteligência artificial e veículos autônomos nos mesmos moldes dos filmes de ficção científica que se vê no cinema e na TV (SOARES, *online*).

Afeito a essa moderna realidade, oportunas são as palavras de Liedke e Schiocchet (2012, p. 125):

> Na sociedade do risco global todos os membros encontram-se expostos a riscos globais, em virtude do desenvolvimento tecnológico, das relações de mercado, das manipulações genéticas, da exploração da biodiversidade, entre outros. Nesse contexto, a proteção jurídica eficaz ao ambiente é submetida a condições de risco reforçadas pelo anonimato, imprevisibilidade e precariedade nas bases de informação para qualquer tomada de decisão.

Por causa do já aludido potencial lesivo proveniente da notória expansão tecnológica, não há como olvidar o uso do princípio da precaução por parte dos países na criação de dispositivos que coloquem em risco os direitos das futuras gerações, como está explícito e detalhado pela própria Comissão das Comunidades Europeias (*online*):

> O princípio da precaução deveria ser considerado no âmbito de uma abordagem estruturada da análise de riscos, a qual inclui três elementos: a avaliação de riscos, a gestão de riscos e a comunicação de riscos. O princípio da precaução é particularmente relevante no que se refere à gestão de riscos.
> O princípio da precaução, que é essencialmente usado pelas instâncias de decisão na gestão de riscos, não deveria ser confundido com o factor de prudência utilizado pelos investigadores na sua avaliação de dados científicos.
> O recurso ao princípio da precaução pressupõe que se identificaram efeitos potencialmente perigosos decorrentes de um fenómeno, de um produto ou de um processo e que a avaliação científica não permite a determinação do risco com suficiente segurança.
> A implementação de uma abordagem baseada no princípio da precaução deveria começar com uma avaliação científica, tão completa quanto possível, e, quando praticável, identificando em cada fase o grau de incerteza científica.

Explicando as possibilidades interpretativas desse princípio, Liedke e Schiocchet (2012, p. 127) afirmam ainda que:

> O princípio da precaução [...] busca implementar as melhores decisões possíveis em estados de incerteza (de conhecimento indisponível, inacessível ou mesmo inexistente). Nesse sentido, os valores exclusivamente científicos devem ser substituídos por outros – ou ao menos relativizados, postos em discussão. Afinal, a realidade técnica e científica são apenas uma dentre outras facetas que os processos de tomada de decisão sobre os riscos engendram atualmente.

Como consequência lógica desses cuidados globais, a manutenção de dados pessoais por terceiros desconhecidos começou a ressonar às autoridades de muitos países como algo potencialmente lesivo, o que gerou um interesse global pela regulação daquele ato, gerando, com isso, o crescimento exponencial das regulamentações sobre tratamento de dados digitais[18], principalmente após a criação da *General Data Protection Regulation – GDPR* da União Europeia, no dia 25 de maio de 2018, substituindo a Diretiva 95/46/EC[19].

Não podendo ser diferente, e seguindo esse fluxo global, o Brasil também criou a sua Lei Geral de Proteção de Dados Pessoais, ratificada no dia 14 de agosto, de 2018, conhecida pela Lei nº 13.709/18.

Embora seja uma lei muito inovadora, e que trará grandes mudanças no tratamento de dados pessoais no cenário nacional, antes de sua criação leis esparsas já sinalizavam o interesse legislativo em cuidar dos dados pessoais das pessoas no Brasil.

Entre esses dispositivos legais, tem-se, lidando direta ou indiretamente com a proteção e tratamento de dados, o próprio Código de Defesa do Consumidor (Lei Federal nº 8.078/90), nos artigos 43, 72 e 73, o Marco Civil da Internet (Lei Federal nº 12.965/14), nos artigos 3º, III; 7º, VII, VII, IX, X; 10; 11; 16, II, o Decreto nº 8.771/16, no capítulo III), a Lei do Cadastro Positivo (Lei Federal nº 12.414/11), no artigo 5º, V, VI e VII, o Decreto do Comércio Eletrônico (Decreto nº 7.962/13), no

---

[18] Dados colhidos em agosto de 2018 (DONEDA, Danilo. *A Lei Geral de Proteção de Dados Pessoais*. XXXVIII Congresso Internacional da Propriedade Intelectual da Associação Brasileira da Propriedade Intelectual – ABPI: agosto de 2018.

[19] Criada em 24 de outubro de 1995. Há de salientar que a internet naquela época era incial, parada a hoje, não existindo conceitos que hoje são tidos como comuns, como nuvem, aplicativos e redes sociais. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046L. Acesos em: 18 set. 2020.

artigo 4º, VII, a Lei de Acesso a Informações (Lei Federal nº 12.527/11), na seção V, além da Lei de Crimes Cibernéticos (Lei nº 12.737/2012), o Marco Civil da Internet (Lei nº 12.965/2014), e o Anteprojeto de Lei de Proteção e Dados Pessoais no Brasil (Lei nº 5.276/2016).

No entanto, uma das manifestações mais diretas para organizar o futuro da proteção de dados no Brasil ocorreu em 2016, a partir da instituição da Política de Governança Digital nos órgãos e entidades da administração pública federal. Nesse momento, houve a elaboração da Estratégia de Governança Digital da Administração Pública Federal (EGD), onde se definiu objetivos estratégicos, metas e indicadores da PGD, formando três eixos, dez objetivos e cinquenta e uma iniciativas estratégicas (EDG, *online*).

Na análise desse documento, se percebe a preocupação mais direta com a proteção de dados pessoais no item 11, intitulado “Iniciativas Estratégicas, Indicadores e Metas”, mais especificamente no seu subitem 11.1, intitulado “Acesso à Informação”. Segundo o documento, às três principais iniciativas do Governo Federal foram:

> [...] Portal da Transparência [...] se transformou numa das primeiras plataformas de governo digital e atualmente, disponibiliza outros dados e informações tais como: salários de servidores, convênios, despesas, receitas, empresas punidas, entidades impedidas de celebrar convênios com a União, dentre outros, alguns dos quais em formato aberto.
> [...] o Portal Brasileiro de Dados Abertos [...] tem 5.200 conjuntos de dados, provenientes de mais de 100 organizações, dos três níveis de governo e dos três poderes.
> [...] Lei de Acesso à Informação (LAI), que promove a transparência das ações de governo, a CGU, como responsável pelo monitoramento da aplicação LAI [...]
> Estas três plataformas estão diretamente relacionadas com os objetivos OE.01 - Fomentar a disponibilização e o uso de dados abertos e OE.02 - Promover a transparência por meio do uso de TIC [...].

Já no que tange a uma iniciativa legislativa mais específica e bem mais detalhada, tem-se a própria Lei Geral de Proteção de Dados brasileira (Lei nº 13.709/18), a qual, além de alterar a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil

da Internet)[20], dispõe sobre o tratamento de dados pessoais, também nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com a finalidade de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (art. 1º).

Noutros termos, a nova lei, que entrará em vigor no dia 03 de maio de 2021[21], propõe a proteção dos dados pessoais, os quais seriam relacionados (BOFF, 2018, p. 133): "[...] à pessoa natural identificada ou identificável, inclusive através de números identificativos, dados locacionais ou identificadores eletrônicos".

Diferente do que se vê no dia a dia na realidade legislativa do Brasil, a tramitação da referida lei pôde ser considerada breve, ainda que o Projeto de Lei já existisse desde 13 de junho de 2012 (PL 4060/2012) e só foi realmente acelerado na Câmara dos Deputados no ano de 2015 (BRASIL, 2012, *online*).

No entanto, se houve quase uma década para o Congresso Nacional aprovar o que virou a Lei Geral de Proteção de Dados Pessoais brasileira, após aprovada, já começaram as tentativas de alterações. Após a sua promulgação, em 2018, surgiu à tramitação da Medida Provisória 869/2019, com regime de tramitação de urgência, posteriormente transformada na Lei Ordinária nº 13.853/2019 (BRASIL, 2018, *online*), com o ponto alto na criação da Autoridade Nacional de Proteção de Dados – ANPD (art. 5º, XIX).

A ANPD é um órgão da administração pública federal, vinculado à Presidência da República, se firmando na responsabilidade de órgão regulador da LGPD. Segundo Frazão (2019, *online*), as principais competências da referida autoridade seriam:

---

[20] Art. 60. A Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet) , passa a vigorar com as seguintes alterações:
"Art. 7º: [...] X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais; (NR)
Art. 16: [...] II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a proteção de dados pessoais." (NR)

[21] Originalmente a Nova Lei Geral de Proteção de Dados entraria em vigor 18 meses após sua publicação, mas com a Medida Provisória nº 959, de 29 de abril de 2020, estendeu a *vactio legis* para a nova data. Disponível em: <http://www.in.gov.br/web/dou/-/medida-provisoria-n-959-de-29-de-abril-de-2020-254499639>. Acesso em: 24 jun. 2020.

> [...] além da competência de fiscalizar e aplicar sanções, os artigos anteriores da presente série destacaram expressamente algumas das várias importantes atribuições da autoridade nacional, dentre as quais as de (i) solicitar aos controladores relatórios de impacto à proteção de dados, (ii) determinar o término do tratamento de dados quando houver violação à lei, (iii) determinar o bloqueio ou eliminação de dados, (iv) receber e se pronunciar sobre reclamações dos usuários e todas as manifestações decorrentes do direito de petição e (vi) realizar auditorias em casos de decisões totalmente automatizadas.

No entanto, além de criar a figura ANPD, não há como esquecer do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, um dos órgãos da sua estrutura organizacional, contando com (SERPRO, online):

> [...] 23 titulares, não remunerados, com mandato de dois anos, e de diferentes setores: seis do Executivo Federal; um do Senado Federal; um da Câmara dos Deputados; um do Conselho Nacional de Justiça; um do Conselho Nacional do Ministério Público; um do Comitê Gestor da Internet no Brasil; quatro da sociedade civil com atuação comprovada em proteção de dados pessoais; quatro de instituição científica, tecnológica e de inovação; e quatro de entidade do setor empresarial ligado à área de tratamento de dados pessoais.

Prosseguindo, a MP 869/2019 ainda contou com mais mudanças importantes. O novo parágrafo 4º, do art. 11, da LGPD, trouxe maiores diretrizes quanto ao uso de dados pessoais por empresas da área da saúde, mais precisamente às que operam com planos de saúde.

No texto original, havia maior rigorosidade quanto à disponibilidade do acesso aos dados dos consumidores pelas companhias de saúde[22]. No texto final, se possibilitou maior flexibilização:

> § 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: I - a portabilidade de dados quando solicitada pelo titular;

22 § 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nos casos de portabilidade de dados quando consentido pelo titular.

> ou II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo.

Numa leitura primária, parece que houve um retrocesso quanto à segurança que os consumidores exigiam para quem detinha o poder sobre seus dados. Porém, para não se afirmar que não houve atenuações nesse possível retrocesso, o parágrafo 5º, do mesmo artigo, trouxe um freio, ao afirmar: “É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.”. Com isso, pelo menos ficará vedado a essas empresas que tracem os dados dos seus clientes para montar perfis de viabilidade econômica no oferecimento dos serviços.

Por fim, importante apontar que, no tocante aos dados tratados coletivamente pelas empresas com intuito de definir apenas perfis de usuários (dados anonimizados), sem a possibilidade de identificá-los, não houve qualquer alteração, mantendo-se o texto original da LGPD (GOMES, online, 2019). Dessa forma, não é necessário o consentimento do usuário consumidor para traçar simplesmente o seu perfil, sendo, portanto, uma exceção, pois, na regra geral, para que os dados pessoais sejam tratados, analisados ou manipulados é necessário o consentimento do titular, como será melhor explicado no capítulo três.

3.1 A Lei Geral de Proteção de Dados brasileira e a Regulamentação Geral de Proteção de Dados da União Europeia como referencial norteador e impositivo ao ordenamento jurídico brasileiro

Ante a visibilidade internacional que foi dada ao Regulamento Geral sobre Proteção de Dados da União Europeia, criado oficialmente em 27 de abril de 2016, sob número 2016/679, e entrando em vigor em 25 de maio de 2018 (EUR-LEX, *online*), a impressão que se pode ter é que somente neste ano surgiram dispositivos legais regulando a proteção de dados pessoais na União Europeia, o que não é uma verdade.

De fato, como bem já asseverava Team (2016, p. 11), a GDPR (sigla em inglês do RGPD) era o último passo para solidificar e estruturar as arestas que

faltavam às regulações de proteção de dados pessoais já existentes, lembrando o que levou à criação de tal regulamento:

> The GDPR is the latest step in the ongoing global recognition of the value and importance of personal information. Although the information economy has existed for some time, the real value of personal data has only become more recently evident. Cyber theft of personal data exposes EU citizens to significant personal risks. Big data analysus techniques enable organisations to track and predict individual behaviour, and can be deployed in automated decision-making. The combination of all these issues, together with the continuing advance of technology and concerns about the misuse of personal data by governments and corporations, has resulted in a new law passed by the EU to clarify the data rights of EU citizens and to ensure an appropriate level of EU-wide protection for personal data.

Muito embora o maior impulso criador de regulamentos que versassem sobre direitos relacionados à intimidade, e, consequentemente, aos dados pessoais, tenham sido criados a partir da década de 1960, antes desta data já era possível encontrar os rudimentos que embasariam as regulações futuras, como o artigo 12 da Declaração Universal dos Direitos do Homem[23], publicado originalmente em 1948, e o artigo 8º do Convênio para Proteção de Direitos Humanos e Liberdades Fundamentais[24], pactuado em Roma, no ano de 1950 (RODRIGUES e RUARO, 2010, p. 167). Figura ainda nesta lista de influências os artigos 17 e 18 do Pacto de Direitos Civis e Políticos[25], firmado em Nova Iorque, mas já no ano de 1966. (OAS, *online*).

Após a criação desses documentos, coincidiu de o mundo entrar de fato numa nova era: a tecnológica. Nos anos de 1970 a internet começa a ser uma realidade que impressiona os mais céticos, crescendo num ritmo muito acelerado, como bem alude Leiner et al. (1995, *online*):

---

[23] Artigo 12: “Ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques a sua honra e reputação. Todo o homem tem direito à proteção da lei contra tais interferências ou ataques.”

[24] 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. [...].

[25] Artigo 17: “§1. Ninguém poderá ser objeto de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra e reputação. §2. Toda pessoa terá direito à proteção da lei contra essas ingerências ou ofensas.”; Artigo 18: [...] §2. Ninguém poderá ser submetido a medidas coercitivas que possam restringir sua liberdade de Ter ou de adotar uma religião ou crença de sua escolha. [...]”.

> In December 1970 the Network Working Group (NWG) working under S. Crocker finished the initial ARPANET Host-to-Host protocol, called the Network Control Protocol (NCP). As the ARPANET sites completed implementing NCP during the period 1971-1972, the network users finally could begin to develop applications.

Além da internet, surge, também, como consequência, um alargamento no uso do processamento de dados, inclusive de pessoas. Junto à esta revolução crescente, aparecem, também, blocos econômicos regionalizados, onde o compartilhamento de dados pessoais toma grandes e necessárias dimensões, adentrando na esfera internacional (MALDONADO, 2019, p.20).

Nesse âmbito, com essa extensão de compartilhamento de dados pessoais se estendendo para além do âmbito nacional, surge, naturalmente, um conjunto de legislações com o intuito de proteger a privacidade dos usuários com certa eficiência.

Assim, em 23 de janeiro de 1970 nasce a Resolução nº 428, da Assembleia Parlamentar do Conselho da Europa, comumente chamada de *Declaration on mass communication media and Human Rights* (Declaração sobre os meios de comunicação em massa e os Direitos Humanos, em tradução livre). Essa resolução também alude os cuidados na proteção da vida privada, mas fazendo um aporte a esta e os meios informáticos, como se extrai do texto do item C.19:

> Where regional, national or international computer-data banks are instituted the individual must not become completely exposed and transparent by the accumulation of information referring even to his private life. Data banks should be restricted to the necessary minimum of information required for the purposes of taxation, pension schemes, social security schemes and similar matters.

Prosseguindo, em 28 de janeiro, de 1981, surge outro documento importante: o Convênio nº 108. Disposto pelo Conselho da Europa, o referido documento é o primeiro a tratar diretamente de dados de caráter pessoal, possuindo no seu título o seguinte texto: “Convenio nº 108 del Consejo de Europa para la protección de las personas con respecto al tratamento automatizado de datos de carácer personal”. Este título acaba sendo praticamente o resumo do art. 1º do referido convênio, se tornando, assim, num texto garantidor à cada país-

membro de que os direitos e liberdades fundamentais relacionados à proteção do tratamento automatizado de dados pessoais estaria protegido por força legal.

Entrando na década de 1990, alguns importantes documentos também apareceram. Porém, para basilar esse trabalho acadêmico e não se perder em regulamentações secundárias, é importante destacar o funcionamento da normativa europeia para se entender qual a diretiva que mais nos interessa. Segundo (RODRIGUES e RUARO, 2010, p. 168):

> [...] no cenário europeu atual, podem ser destacadas duas fontes principais de direito: as primárias, que se identificam com os atos jurídicos criadores de regras, previamente pactuadas pelos Estados-membros, e as derivadas, que são regulamentos, diretivas, decisões, recomendações e ditames. [...] as diretivas comunitárias [...] se caracterizam por seu poder vinculante aos Estados integrantes da União Europeia quanto ao resultado, sendo permitido, no entanto, que cada nação escolha a melhor forma de alcança-lo.

Esse esclarecimento é importante porque não há como deixar de analisar uma das diretivas comunitárias mais importantes do Parlamento Europeu e do seu Conselho: a 95/46/1995, que regula a proteção de dados singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Como aludido, por ser uma diretiva comunitária, acabou por estabelecer o dever de os Estados-membros criarem seus códigos de condutas tanto nacionais, quanto comunitárias, de modo que viabilizassem a plena efetividade da diretiva.

Como asseverou Doneda (2006, p. 238), muito embora aquela norma não tenha apontado direitos atinentes à proteção de dados pessoais e seus limites, como fez a RGPD, pelo menos apresentou princípios observáveis nas legislações internas, para que viabilizasse a proteção dos direitos protegidos, como é possível extrair da análise do seu artigo 3º:

> 1. A presente directiva aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos num ficheiro ou a ele destinados.
> 2. A presente directiva não se aplica ao tratamento de dados pessoais:
> - efectuado no exercício de actividades não sujeitas à aplicação do direito comunitário, tais como as previstas nos títulos V e VI do Tratado da União Europeia, e, em qualquer caso, ao tratamento de dados que tenha como objecto a segurança pública, a defesa, a segurança do Estado (incluindo o bem-estar económico do Estado quando esse

> tratamento disser respeito a questões de segurança do Estado), e as actividades do Estado no domínio do direito penal,
> - efectuado por uma pessoa singular no exercício de actividades exclusivamente pessoais ou domésticas.

Dois anos depois, surge a Diretiva 97/66CE, direcionando o tratamento de dados pessoais à proteção da privacidade no setor das telecomunicações (art. 1º). O próprio artigo 2º da diretiva deixa claro que ela é, na verdade, um complemento da diretiva anterior, elencando algumas medidas de segurança em determinados setores. Nesta feita, assegura que havendo violação da segurança nos serviços de telecomunicações disponíveis ao público, o fornecedor responsável é obrigado a informar a ocorrência aos assinantes e as soluções que serão adotadas, incluindo aqui os custos de eventuais reparações.

Finalmente, em 2002, foi promulgada uma das Diretivas mais aguardadas: a 2002/58/CE, tratando da regulamentação da proteção de dados pessoais no âmbito da comunicação eletrônica. Embora não tenha havido inovação de fato ao ordenamento da comunidade europeia, tal regulamentação permitiu a viabilização das finalidades presentes na Diretiva 96/46/CE a uma realidade tecnológica ainda não presente na ocasião da sua promulgação (DONEDA, 2006, p. 239).

Por fim, aponta a Diretiva 2006/24/CE, que seria o mais próximo do que se conhece hoje por tratamento de dados. Nos termos do seu artigo 1º (EUR-LEX, *online*):

> 1. A presente directiva visa harmonizar as disposições dos Estados-Membros relativas às obrigações dos fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações em matéria de conservação de determinados dados por eles gerados ou tratados, tendo em vista garantir a disponibilidade desses dados para efeitos de investigação, de detecção e de repressão de crimes graves, tal como definidos no direito nacional de cada Estado-Membro.
> 2. A presente directiva é aplicável aos dados de tráfego e aos dados de localização relativos quer a pessoas singulares quer a pessoas colectivas, bem como aos dados conexos necessários para identificar o assinante ou o utilizador registado. A presente directiva não é aplicável ao conteúdo das comunicações electrónicas, incluindo as informações consultadas utilizando uma rede de comunicações electrónicas.

Importante observar a ressalva contida no art. 4º da mesma diretiva. Segundo o dispositivo legal, os dados aludidos no artigo 1º só poderão ser

transmitidos às autoridades nacionais competentes em casos específicos, respeitando a necessidade e proporcionalidade, e sempre elencado à legislação nacional vigente (*idem*).

Essa saga de legislações de proteções de dados pessoais se consolida, de fato, em 2016, quando a União Europeia cria o seu Regulamento Geral.

Como era de se esperar, ante o histórico crescente de proteção advindas das legislações anteriores já explicitadas, a nova regulação europeia veio com o intuito de regular a quantidade e qualidade de dados coletados na era digital, tendo em vista a preocupação em proteger a privacidade das pessoas com maior comprometimento, acabando por se tornar uma referência também para o legislador brasileiro quando da codificação da sua lei de proteção de dados pessoais (MALDONADO, 2019, p. 21).

Saliente-se que além dessa evolução legal natural, a razão factual que motivou o aparecimento de uma legislação mais sólidas sobre a proteção de dados foi justamente o próprio avanço da economia digital inserido ao modelo de negócios, que agora passa a usar muito mais os fluxos internacionais de bancos de dados com ênfase aos dados relacionados às pessoas, como consequência dos avanços da tecnologia e da informação. (PINHEIRO, 2018, p. 17).

Porém, embora sejam legislações distintas, formalmente falando, a LGPD e a GDPR possuem algumas semelhantes importantes de serem observadas. Pinheiro (2018, p. 38), ao analisar essa possível comparação, fez a seguinte síntese:

> Considerando a comparação entre LGPD e GDPR, ambas legislações têm como objetivo o regramento do tratamento de dados pessoais, buscando em si a defesa dos direitos fundamentais, buscando em si a defesa dos direitos fundamentais da pessoa natural.

Vê-se, também, que as preocupações que deram abertura ao texto legal da LGPD brasileira (art. 1º[26]) guarda uma correlação clara com a GDPR (*online*):

> Art. 1 GDPR

[26] 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.

> Subject-matter and objectives
> 1.This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
> 2.This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

Outra semelhança interessante é que na LGPD a garantia dos direitos dos titulares dos dados pessoais é norteada por princípios de direitos fundamentais, o que também ocorre com a GDPR, trazendo em seu artigo 5º princípios que embasam o tratamento de dados pessoais (PINHEIRO, 2018, p. 62).

No entanto, sem qualquer demérito por ter buscado se adequar à lei geral da União Europeia, a nova LGPD brasileira visou, também, regulamentar as atividades atualmente conhecidas que envolvam utilização de dados pessoais, sejam feitas por pessoa jurídica ou natural, em território brasileiro ou no estrangeiro, seja no meio físico ou no meio digital, consolidando algumas diretrizes que servirão de guia para a o tratamento dos dados pessoais dos cidadãos consumidores no dia a dia (OLIVIERI, 2019, online).

Além desses aspectos gerais, a LGPD ainda reconhece a tutela dos dados e informações dos consumidores para a proteção de alguns direitos, como os relacionados à privacidade, autodeterminação informativa, liberdade de expressão, de informação, de comunicação e de opinião, inviolabilidade da intimidade, da honra e da imagem, o desenvolvimento econômico e tecnológico e a inovação e a livre iniciativa, a livre concorrência e a defesa do consumidor, como explicitado no artigo 2º; sem esquecer o seu inciso VII, o qual fundamenta os Direitos Humanos Fundamentais como justificativa para a tutela dos dados pessoais (MULHOLLAND, 2018, p. 162, online).

Como consequência dessa nova legislação, não há como olvidar os importantes impactos que ela produz tanto no âmbito social, quanto no econômico, principalmente se for considerada à necessidade de adaptações das pequenas empresas e startups. Meditando sobre esses impactos, Pinheiro (2019, p. 321) observa:

> Tanto por que traz exigências que aumentam os custos empresariais e passam a ter que entrar na prioridade dos gestores (*road map*) mas como também exigem alguns processos de governança corporativa (de TI, de Segurança de Informação, de

> Gestão de Dados) que não eram tão comuns neste ambiente e que podem até dificultar (burocratizar) suas atividades que estão mais acostumadas com leveza e velocidade.

Analisando esse mesmo fenômeno dos impactos econômicos, com a visão voltada para outra senda de raciocínio, mas que complementa o raciocínio acima, Bárbara Pinheiro et al. (p. 22, *E-book*) constrói a seguinte observação:

> A LGPD impactará ou já está impactando profundamente em todos os setores da economia, trazendo modificações [...] inclusive extraterritorialmente, quando especifica que todas as operações de coleta e/ou tratamento dos dados pessoais realizados no Brasil que visem a oferta de bens ou serviços em nosso território ou que tenha por objeto dados de brasileiros estarão sujeitas à lei. As empresas, portanto, independentemente de gerenciarem as informações coletadas através do arquivamento de documentos físicos ou de sistema digitais, deverão se adaptar aos novos padrões de segurança e de privacidade sob pena de

Em contrapartida, é inegável que uma importante inovação presente com a chegada da LGPD é a ampliação do conceito de dados pessoais e a importância de a operação de tratamento de dados ter uma base legal. Noutros termos, nas palavras de Doneda e Mendes (2018, p. 582):

> A grande inovação que a LGPD operou no ordenamento jurídico brasileiro pode ser compreendida na instituição de um modelo *ex ante* de proteção de dados, baseado no conceito de que não existem mais dados irrelevantes diante do processamento eletrônico e ubíquo de dados na sociedade da informação. Os dados pessoais são projeções diretas da personalidade e como tais devem ser considerados. Assim, qualquer tratamento de dados, por influenciar na representação da pessoa na sociedade, pode afetar a sua personalidade e, portanto, tem o potencial de violar os seus direitos fundamentais.

Por ter surgido no momento histórico que mais se viu a criação de regulações de proteção de dados pelo mundo e, principalmente, por ainda não ter entrado em vigor, surge, evidentemente, uma série de discussões quanto a eficácia da Lei Geral de Proteção de Dados. Legislações dessa envergadura abalam grandemente os alicerces de hábitos empresariais, e não basta simplesmente escrever no texto legal o que deverá se fazer, ou não, para que se produza efeitos práticos.

Quando se fala de eficácia se está buscando o enquadramento de determinado dispositivo legal na realidade prática do país, a qual, nas palavras de Bárbara Pinheiro el al. (p. 18, *E-book*) tem de ser analisada nos seguintes contornos:

> [...] quando o assunto é eficácia de uma legislação, [...] alguns itens devem ser levados em consideração, como por exemplo, a quantidade de utilização daquela lei nos julgados brasileiros; a repercussão e discussão sobre a temática dentro da sociedade em que a lei está inserida; os efeitos causados nas empresas daquela sociedade; as sanções trazidas pelo "andar" em desconformidade com a lei; a utilização dela como referência para formação ou criação de estatutos, contratos, e demais documentos considerados necessário a formação de uma pessoa jurídica, etc.

Porém, um ponto chama a atenção e ganha destaque no debate internacional sobre o alcance das regulações sobre proteção de dados pessoais. Tanto na LGPD, quanto na GDPR, tem-se que a garantia de proteção dos dados pessoais das pessoas, por ganharem um relevo de status de princípios de direitos fundamentais, poder-se-ia criar um efeito cascata sobre possíveis tratados internacionais que versasse sobre direitos humanos.

Não há como fechar os olhos à realidade crescente no mundo de criar uma coalisão global sobre assuntos que tratam de direitos humanos. É nessa esteira que Maués (2013, p. 219, *online*) explica essa tendência que já foi apreciada pelo próprio Supremo Tribunal Federal:

> [...] a tendência contemporânea do constitucionalismo mundial de prestigiar as normas internacionais destinadas à proteção dos direitos humanos, a evolução do sistema interamericano de proteção dos direitos humanos e os princípios do direito internacional sobre o cumprimento de obrigações internacionais não permitiam mais a manutenção da tese da legalidade, servindo a supralegalidade como uma solução que viria compatibilizar a jurisprudência do STF com essas mudanças, sem os problemas que seriam decorrentes da tese da constitucionalidade. Assim, os tratados de direitos humanos passam a paralisar a eficácia jurídica de toda e qualquer disciplina normativa infraconstitucional com eles conflitante.

Essa abertura da Constituição Federal à normação internacional está alinhada ao processo de globalização que permeia o mundo. Como efeito desse

raciocínio, há a ampliação do "bloco de constitucionalidade"[27], que passa a incorporar preceitos assecuratórios de direitos fundamentais (PIOVESAN, online). Exemplo disso é a força impositiva proposta aos tratados internacionais, como bem alude a Convenção de Havana sobre Tratados, firmada em 1928, sendo promulgada no Brasil sob o Decreto n. 5647/29, a qual explicita, no seu artigo 11 que:

> Los Tratados continuarán surtiendo sus efectos aún cuando llegue a modificarse la constitución interna de los Estados contratantes. Si la organización del Estado cambiara de manera que la ejecución fuera imposible, por división de territorio o por otros motivos análagos, los tratados serán adaptados a las nuevas condiciones.

Nessa mesma linha impositiva, a Convenção de Viena sobre Direito dos Tratados, de 1969, afirma em seus artigos 26 e 27, respectivamente:

> 26. **"Pacta sunt servanda".** Todo tratado en vigor obliga a las partes y debe ser cumplido por ellas de buena fe.
> 27. **El derecho interno y la observancia de los tratados.** Una parte no podrá invocar las disposiciones de su derecho interno como justificación del incumplimiento de un tratado. Esta norma se entenderá sin perjuicio de lo dispuesto en el artículo 46. (Grifos originais).

Nessa esteira legal, se o Estado signatário se submeter às normas internacionais e por algum motivo não fazer jus a confiança depositada, estaria praticando uma espécie de ato ilícito, se sujeitando a uma reparação internacional.

Esses tratados internacionais versando sobre a proteção de dados pessoais ainda não existem na realidade, só existindo sua possibilidade no plano teórico. Todavia, há quem critique justamente isso, a ausência de uma norma que seja um guia para os países. Nas palavras de Pinheiro (2019, p. 321):

> Apesar de vivermos uma sociedade globalizada, da internet ser um grande território internacional e de se querer permitir o livre fluxo de dados, em matéria de proteção de dados pessoais acabou-se utilizando os mecanismos das leis nacionais e dos regulamentos

[27] Segundo Vargas (2007, p. 12, online): "[...] a palavra "bloco" significa algo sólido, duro, compacto, um conjunto de coisas consideradas como uma unidade. Fazendo a junção do termo bloco com a expressão Constituição, e em razão da própria definição de bloco, é possível extrair que Bloco de Constitucionalidade é algo como um conjunto de normas constitucionais consideradas em sua unidade.

> regionais, e esta é a maior crítica que se pode ter quanto ao desdobramento que se teve deste assunto.

Mesmo que a globalização legal seja uma realidade irreprochável, e, portanto, por meio dos tratados internacionais seja possível a imposição de novas diretrizes à Lei Geral de Proteção de Dados brasileira, não há como olvidar que no inciso I, do artigo 1º, da Constituição Federal, de 1988, afirma que a República Federativa do Brasil tem como princípio fundamental a soberania, e no inciso I, do artigo 4º, afirma que o Brasil irá reger as relações internacionais com independência nacional.

Nesta feita, com todo respeito às ideias defendidas nos ordenamentos jurídicos de âmbito global, não há como separar da discussão a supremacia formal e material da Constituição Federal sobre o ordenamento jurídico pátrio. Cada país possui particularidades que acabam sendo tão peculiares que não suportariam ordenamentos globais que não fossem aportes tão somente de preceitos gerais. Pensar diferente e aceitar a submissão do País aos tratados internacionais para além do poder constitucional, seria, ao nosso ver, um impedimento prático, inclusive, à realização do controle de constitucionalidade dos próprios tratados.

3.2 As principais exigências ao tratamento de dados pessoais sensíveis e seus desafios interpretativos

Conceituar os dados pessoais seria o primeiro passo para se direcionar a norma em análise, estabelecendo limites de proteção à tutela jurídica pretendida. Não são todos os dados que teriam uma repercussão jurídica, mas somente aqueles que de alguma forma atraísse o qualificador pessoal (BIONI, 2019, p. 101, *E-book*).

Segundo conceituação da Comissão Europeia na GDPR: “Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.” (EUROPEAN COMMISSION, *online*).

Nos termos da Lei Geral brasileira (art. 5º, I), o conceito de dados pessoais é bem singelo, afirmando tão somente ser (BRASIL, *online*) “informação relacionada a pessoa natural identificada ou identificável”.

Um conceito simplório tem suas qualidades e malefícios. No caso da conceituação de dados pessoais parece se necessitar com maior ênfase dos esforços doutrinários para estender um pouco mais o alcance interpretativo de tal conceito.

Dados pessoais são fatos, comunicações e ações referenciadas a circunstâncias pessoais ou materiais de um indivíduo identificado ou identificável. O indivíduo é considerado identificável quando pode ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social. (MENDES, 2014, p.55).

Noutros termos, um dado será considerado pessoal quando trouxer elementos que possibilitam a identificação, direta ou indireta, da pessoa natural por trás do dado, como, por exemplo, nome, sobrenome, data de nascimento, documentos pessoais (como CPF, RG, CNH, Carteira de Trabalho, passaporte e título de eleitor), endereço residencial ou comercial, telefone, e-mail, cookies e endereço IP (BOFF, FORTES e FREITAS, 2018, p. 105).

Na visão de Castro (2002, *online*), em meados de 2002 já se acreditava que um conceito de dados não poderia se limitar ao que ele chama de informações pessoais diretamente consideradas:

> Ao cogitarmos dos dados pessoais constantes de bancos, não podemos nos limitar às informações pessoais diretamente consideradas, como nome, data de nascimento, filiação etc. As leis referidas consideram também objeto de proteção todo tipo de informações que indiretamente possam ser associadas a uma pessoa, por exemplo, um número de telefone, uma placa de automóvel, um endereço de e-mail. Constituem dados de caráter pessoal toda informação (ainda que anônima) com a qual se possa, mediante associações e cruzamento de dados, identificar-se uma pessoa, como o DNA, a impressão digital ou dados incompletos de um indivíduo.

Claramente essa visão de Castro ainda é primária, frente aos detalhamentos de espécies de dados que a própria LGPD fez, mas mesmo assim revela que de alguma forma todos os dados podem estar interligados.

Na visão de Bioni (2019, p. 101-102, *E-book*), o vocabulário para prescrever a proteção dos dados pessoais segundo a LGPD pode ser confundida por "[...] uma bipartição do seu léxico que ora retrai (reducionista), ora expande (expansionista), a moldura normativa de uma lei de proteção de dados pessoais.". Ainda segundo sua visão (*idem*), o léxico expansionista teria como elementos: 1) pessoa identificável; 2) pessoa indeterminada; 3) vínculo mediato, indireto, impreciso ou inexato; 4) alargamento da qualificação do dado pessoal. Em contrapartida, o léxico reducionista teria como elementos: 1) pessoa identificada; 2) pessoa específica/determinada; 3) vínculo imediato, direto, preciso ou exato; 4) retração da qualificação do dado como pessoal.

Ao analisar esses mesmos léxicos, Oliveira (2018, p. 256) observou que a LGPD adotou a definição expansionista, ou seja "[...] dados que inicialmente não identificam uma pessoa (como endereço IP, faixa etária, nacionalidade etc.), ao serem conjugados ou enriquecidos, se puderem identificar uma pessoa, serão considerados dados pessoais."

Na visão de Bioni (2019, p. 103, *E-book*), conceituar dados pessoais tem que ter uma definição fluída e dinâmica, atraindo conceitos básicos de sistemas de informação e de bancos de dados:

> A intelecção do conceito de dado pessoal e, por conseguinte, das estratégias regulatórias possíveis para a sua definição é algo fluido, que pode ser esclarecido a partir da dinâmica de conceitos básicos de sistemas de informação e de banco de dados. Somente, assim, o seu vocabulário ganhará uma análise mais concreta a demonstrar as diferenças e consequências práticas entre tais estratégias regulatórias distintas.

Já quanto ao dado sensível, que é uma espécie do dado pessoal, o inciso II, do art. 5º, é mais detalhado, afirmando ser aquele: [...] 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.

Segundo Doneda (2019, p. 35-54), todos os dados sensíveis são dados pessoais, mas o contrário não poderia ser dito. Indo mais além, alude, ainda, que

a violação a dados sensíveis traz repercussão mais severa à personalidade do indivíduo, dando causa à discriminação, nos casos de mau uso de tais dados.

Nessa esteira, os dados sensíveis seriam (FERREIRA e RODRIGES, 2019, p. 197): [...] aqueles que possuem um potencial discriminatório de maior escala, como convicção religiosa, opinião política e organização genética.

Observe-se que o campo de alcance da proteção dos dados sensíveis dá ensejo as mais variadas particularidades que podem, inclusive, extrapolar as próprias espécies de dados sensíveis contidos no dispositivo legal. Dessa feita, para Korkmaz e Negri (2019, online), seria interessante estruturar tais dados como se fossem uma espécie de cláusula geral:

> No caso do regime normativo dos dados sensíveis, a determinação de eixos específicos de qualificação jurídica acabaria por "filtrar" variadas situações nas quais a dilatada potencialidade lesiva que a tecnologia apresenta no tocante ao tratamento de certos dados restaria desconsiderada, entregando - se à proteção ao regime comum da LGPD, apesar da aptidão de gerar práticas preconceituosas, notadamente em face do mercado.
> Com efeito, a partir da consideração da precariedade de uma normativa fechada em núcleos de *fattispecie*, uma vez verificada a complexidade das manifestações da personalidade que podem ensejar situações de discriminação e desigualdade, aponta-se para uma tutela dos dados sensíveis que se estruture de forma análoga a uma cláusula geral, sob pena da disciplina jurídica, *per se*, não se dar de forma isonômica. É essa natureza do tratamento normativo que se pretende avaliar na LGPD. (Grifos originais).

Os setores empresariais que tenham ambição de lidar com esses tipos de dados deverão se adequar mais ainda a nova legislação, uma vez que somente se poderá fazer sua lida quando o titular ou responsável legal consentir, de forma específica e destacada, para finalidades bem definidas previamente. Como alude Santos e Taliba (2018, p. 230):

> [...] o consentimento para coleta de dados (quando a lei assim exigir) deve ser livre, informado e inequívoco. Já o consentimento, em se tratando de dados sensíveis, deve ser livre, informado, inequívoco, específico e muito bem destacado

No entanto, como forma de relativização à regra contida na lei objeto do presente estudo, nem sempre será necessário o consentimento do consumidor para efetuar a coleta dos dados. De forma sistemática, Santos e Taliba (2018, p.

230), concluindo o raciocínio do parágrafo anterior, e fazendo uma síntese do inciso II, do art. 11, da LGPD, apontam as possíveis exceções:

> [...] a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos; e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistema eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Outro ponto que merece destaque, e que também está relacionado aos dados pessoais é a questão do tratamento de tais dados.

A Lei Geral protege situações que concernem exclusivamente a operação intitulada tratamento de dados, isto é, segundo o artigo 5º, inciso X:

> [...] toda operação realizada com dados pessoais, com as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

Atrelado a esse artigo, tem-se o art. 6º, com os princípios norteadores do tratamento de dados, indicando no caput o da boa-fé como referencial e apontando os seguintes princípios nos seus incisos: (i) finalidade; (ii) adequação; (iii) limitação do tratamento de dados ao mínimo necessário para a realização de suas finalidades; (iv) garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; (v) qualidade dos dados, ou seja, garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados; (vi) transparência; (vii) segurança; (viii) adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; (ix) impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; e (x) responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes

de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Na visão de Santos e Taliba (2018, p. 227-228), dos princípios da boa-fé e da segurança decorrem os demais princípios que deverão guiar o comportamento das empresas que coletam e tratam, de qualquer forma, dados pessoais, se destacando o seguinte raciocínio:

> (i) minimização dos dados – não estamos mais na era da coleta irrestrita de dados. Os princípios da Lei impõem, que sejam coletados apenas dados mínimos para a finalidade do serviço a ser prestado ou produto. Isso se aplica, também, às autoridades, ainda que, nesses casos, se dispense o consentimento expressp do tratamento (art. 7º). Esse conceito deve ser incorporado desde a concepção do serviço ou produto a ser ofertado (*Privacy by Design*), devendo o controlador sempre efetuar a pergunta "é preciso coletar esse dado? Para qual finalidade"?, na medida em que, inexistindo finalidade clara e adequação, o tratamento poderá ser considerado abusivo; (ii) adequação do tratamento dos dados à finalidade para os quais foram coletados – na mesma esteira da minimização, ainda que a hipótese seja a da dispensa do consentimento inequívoco, os dados deverão ser utilizados apenas para as finalidades específicas para as quais foram coletados e devidamente informadas aos titulares, e o tratamento não pode estar dissociado daquilo que o titular razioavelmente esoera ao fornecê-lo.

Continuando na temática da segurança no procedimento do referido tratamento, há de se destacar o texto escrito no inciso VII, do art. 6º, da LGPD, o qual diz respeito à "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão."

No que diz respeito a essas medidas técnicas, impossível não se vincular a matéria à Tecnologia da Informação, onde se encontra recursos oriundos da área da informática munidos de ferramentas e funcionalidades capazes de garantir a segurança da informação. Na visão de Maldonado (2019, p. 329), são exemplos de tais medidas:

> [...[ferramentas de autenticação de acesso a sistemas, mecanismos de segurança em softwares e hardwares, recursos de controle de tráfego de dados em rede, instrumentos detectores de invasões de sistemas, recursos de criptografia, segregação de servidores, ferramentas de prevenção à perda de dados, testes de vulnerabilidade, cópias de segurança, entre muitos outros.

Em contrapartida, tem-se as medidas administrativas, que seriam os procedimentos adotados na esfera gerencial dos agentes de tratamento, somando-se a essas as de natureza jurídica. Ainda segundo Maldonado (2019, p. 330), são exemplos dessas medidas:

> [...] políticas corporativas para proteção de dados pessoais, contratos de confidencialidade, política de privacidade de sites e aplicativos, capacitação dos empregados cujas atividades envolvam o tratamento de dados pessoais, controle de acesso aos arquivos físicos, entre outras.

Assim, é possível usar as palavras de Mendes (2014, p. 94) para sintetizar o seguinte conceito:

> O tratamento abarca, portanto, a realização de inúmeras atividades, como a coleta, o registro, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, o pagamento ou a destruição.

Nesse diapasão, com o que até aqui já foi ventilado, é possível afirmar que o âmbito de aplicação da LGPD se limita a operação de tratamento de dados pessoais que tenham ocorrido nos limites do território brasileiro ou que possuam, de alguma forma, como intuito final, a oferta de bens ou serviços a consumidores que estejam no Brasil, ainda que tenham sido coletados por meios físicos ou digitais, *off-line* ou *on-line*. Ferreira e Rodrigues (2019, p. 196) explicando estes tipos de coletas, afirma:

> O dados pessoais coletados *on-line* são aqueles que valem de métodos automatizados, normalmente preenchidos por uma pessoa em protocolados na internet, por meio de redes sociais, aplicativos, ou contratação de serviços. A coleta de dados *off-line* ocorre pela obtenção destes sem utilizar processos automatizados, seja do preenchimento de pesquisas de intenção, seja por meio de cadastro de clientes de uma determinada empresa. (Grifos originais).

No entanto, dá pra se afirmar que todo esse processo do tratamento de dados exige uma estrutura operacional que pode ir para além do simples armazenamento em servidores. Atualmente já existem técnicas sofisticadas aptas a fazerem a mineração dos dados, como é o caso da *data warehousing,* que

significa, literalmente, depósito de dados, e que seria, nas palavras de Mendes (2014, p. 108):

> [...] um sistema informatizado que armazena enorme quantidade de informações e está organizado de tal modo a facilitar a extração de relatórios, o exame de grandes volumes de dados, bem como a tomada de decisão.

A exploração do *data warehouse* pode ser operada através de inúmeras técnicas, sendo uma delas o *data mining.* Ainda segundo Mendes (2014, p. 108), esta técnica consiste:

> [...] o processo pelo qual dados de difícil compreensão são transformados em informações úteis e valiosas para a empresa, por meio de técnica informática de combinação de dados e de estatística. Isso significa que, por meio de uma única tecla, empresas são capazes de unir e combinar dados primitivos de uma pessoa, formando novos elementos informativos.

A partir dessas informações, se vê que a finalidade de mineração dos dados é gerar regras para classificar pessoas ou objetos. No entanto, não há como deixar de perceber, também, que essa técnica de mineração dos dados pode colidir com a proteção de dados pessoais. Desse modo, como já aludido, a utilização da técnica para ser considerada legítima, necessitará do prévio consentimento do consumidor, em prol da transparência das finalidades, de modo que o usuário possa ser informado dos objetivos da coleta.

Porém, uma observação foi apontada por Santos e Taliba (2018, p. 228) de forma muito pertinente quanto a questão desse consentimento:

> [...] é indubitável que o consentimento será considerado nulo, caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca. Ainda, qualquer alteração da finalidade da coleta deverá ser objeto de consulta e, se o caso, novo consentimento do titular, pois o princípio da finalidade será relacionado com a privacidade informacional e, na hipótese de alteração, o titular pode não concordar com o novo caminho que seus dados percorrerão, o que violaria a autodeterminação informativa.

Muita embora o artigo 5º, inciso X, traga um rol descritivo das possibilidades do tratamento de dados, o que, claramente, gera uma limitação de

atuação por força de lei, o que também merece destaque são as exceções, ou seja, a não necessidade de fazer tratamento de dados. Essas exceções estão elencadas taxativamente no artigo 4º, da LGPD, quando:

> I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
> II - realizado para fins exclusivamente: a) jornalístico e artísticos; ou b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
> III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; ou
> IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

Diante de tudo que já foi apontado até agora, não há como não questionar a relação entre os dados pessoais sensíveis e o tratamento de dados ao tratamento de dados pessoais sensíveis do setor da saúde, principalmente por esse o objeto de estudo desse trabalho.

Como já apontado no primeiro capítulo, os dados pessoais sensíveis das pessoas estão sendo um produto muito lucrativo para empresas da saúde que os utiliza para cruzar informações para produção de medicamento e tratamentos, embora, como também apontado, sem autorização do paciente e, as vezes, com fins escusos que constantemente são objetos de investigações. Porém, para além do viés econômico, também é possível identificar o desafio de coletar, processar, analisar, enfim, fazer o devido manuseio dessa espécie de dados pessoais.

No artigo 11, da LGPD, o tratamento de dados sensíveis ganha enfoque direcionado, com seção própria, apontando que ele só poderá ser feito nas seguintes hipóteses:

> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

É nesse cenário de ajuste técnico e administrativo do tratamento de dados sensíveis que a Organização Pan-Americana da Saúde (2018, p. 12) chama a atenção para os cuidados que os países deverão ter para lidar com a manipulação de tais dados:

> Os países, além de superar o desafio de universalizar e ampliar a qualidade da infraestrutura das TIC nos estabelecimentos de saúde, também precisam desenvolver as competências e habilidades digitais necessárias para seu uso entre os profissionais e gestores de saúde. Os prontuários médicos eletrônicos, a tecnologia móvel em saúde (m-Saúde), os dispositivos vestíveis (wearables), os serviços de telessaúde, teleconsulta, telemedicina e o manejo de enormes bases de dados (big data) hospitalares e de ferramentas de análise de dados (data analytics) são apenas alguns dos exemplos de uso das TIC em saúde que exigem novas competências e habilidades digitais.

Esses cuidados podem parecer exagerados e pouco práticos para tratar dados que no cotidiano nem de perto passam por esse controle. A questão é que informações do setor da saúde por terem recebido status de direito fundamental, guardam no seu bojo um potencial lesivo sobre todos aquelas espécies de dados simplesmente pessoais já elencadas. Na visão de Lima et al. (2019, p. 53, *E-book*).

> Os dados sensíveis possuem informações que podem gerar grande exposição na vida social e profissional do seu titular, sendo assim, para respeitar a privacidade e garantir que eles não sejam utilizados contra os próprios titulares gerando restrições ao acesso de serviços e bens, o tratamento desses dados deve ser feito com muito rigor e cautela à luz do artigo 11 da Lei Geral de Proteção de Dados Pessoais (LGPD). Se não existir um tratamento diferenciado, dados importantes como biometria, imagens faciais, impressões digitais e dados físicos e psicológicos podem gerar grande risco de discriminação por parte dos planos de saúde, por exemplo.

Uma dúvida que poderia surgir seria sobre o tráfego de dados sensíveis entre setores de planos de saúde e seguros de saúde que ainda hoje é uma atividade praticada, como já explicado no primeiro capítulo. Tomando cuidados quanto a isso, a própria LGPD apontou algumas diretrizes, nos parágrafos 3º, 4º e 5º, do artigo. 11:

> § 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.
> § 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: I - a portabilidade de dados quando solicitada pelo titular; ou II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo.
> § 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários

Por isso, a Lei Geral, no artigo 38, alude sobre a figura da Autoridade Nacional, apontando que ela poderá determinar ao controlador que “[..] elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados [...]”, devendo conter, nos termos do parágrafo único do mesmo artigo, “[...] a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de riscos adotados”.

Saliente-se, ainda, que frente a necessidade da adoção de medidas de segurança, sejam técnicas e administrativa, a Autoridade Nacional poderá, ainda (LIMA el al., 2019, p. 56, *E-book*):

> [...] impor padrões técnicos mínimos, dependendo da natureza das informações, das características específicas do tratamento e do estado atual da tecnologia. Ocorrendo um incidente, ela ainda pode determinar a adoção de providências, tais como a ampla

> divulgação do fato em meios de comunicação; e medidas para reverter ou mitigar os efeitos do vazamento.

Destarte, a LGPD trará grandes e importantes mudanças no setor da saúde no que diz respeito ao tratamento de dados sensíveis, principalmente porque não será admitido operar o tratamento de dados com interesses diversos daqueles consentidos pelos titulares dos dados. Com isso, às empresas do setor da saúde que farão o tratamento de dados sensíveis de seus pacientes/consumidores devem assegurar as medidas de segurança necessárias para evitar que terceiros não autorizados possam ter acesso ao conteúdo dos dados confiados.

5 O PROGRAMA DE COMPLIANCE COMO ESTRATÉGIA NO TRATAMENTO DE DADOS SENSÍVEIS NA ÁREA DA SAÚDE

A economia global passa um período de transição muito empolgante e ao mesmo tempo muito desafiador. No momento em que as relações interpessoais virtuais ganham notoriedade, da mesma forma as empresas espalhadas pelo mundo buscam um maior estreitamento tecnológico entre si, sem perderem de vista à segurança nas suas transações e investimentos.

Sempre que um escândalo de corrupção rompe no mundo, uma onda de insegurança brota nos investidores, como se constata de forma muito clara, por exemplo, na oscilação instantânea que ocorre nas bolsas de valores globais.

Frente a isso, medidas de governança corporativa estão sendo cada vez mais implementadas na própria estrutura das empresas a fim de as ajudarem com as demandas de segurança e solidez notoriamente requeridas pelos consumidores e investidores.

No Brasil, existe o chamado Instituto Brasileiro de Governança Corporativa (IBGC), o qual, segundo suas próprias palavras (IBGC, *online*):

> [...] é uma organização sem fins lucrativos, referência nacional e internacional em governança corporativa. O instituto contribui para o desempenho sustentável das organizações por meio da geração e disseminação de conhecimento das melhores práticas em governança corporativa, influenciando e representando os mais diversos agentes, visando uma sociedade melhor.

Nessa esteira, agora tratando sobre o que seria de fato a Governança Corporativa, a IBGC (*online*) também tem um conceito:

> Governança corporativa é o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas.

Esse conceito é um bom ponto de partida, mas incompleto. Numa primeira vista, parece que governança se limitaria a simples imposição de regras, o que, na verdade, não seria condizente com o *animus* na criação de tais diretrizes. Desse modo, fazendo uma complementação ao conceito acima, buscando fazer

uma análise da governança na perspectiva das garantias e efeitos práticos em favor dos agentes envolvidos, Godoi (2020, *E-book*) alude:

> A governança corporativa visa garantir que os agentes de governança nas empresas atuem de maneira ética nas decisões corporativas a fim de maximizar a expectativa de retorno econômico para os investidores e a geração de valor de longo prazo para o próprio negócio e demais partes interessadas que se relacionam com a empresa ou que por ela são afetadas. Para tal, promove o estabelecimento de normas, recomendações, princípios e regras de boas práticas de governança corporativa.

Muito embora seja um termo muito utilizado nos dias atuais, a governança corporativa já estava sendo utilizada, ainda tímida e de diversas formas, já na década de 1990, principalmente após grandes escândalos ocorridos na década anterior, fatos estes que fizeram com que as grandes companhias já se antecipassem na criação de algum tipo de governança, como bem explica o IBGC (*online*):

> As discussões envolvendo acadêmicos, investidores e legisladores, originando teorias e marcos regulatórios, avolumaram-se nos anos 1990, após os graves escândalos contábeis da década anterior, envolvendo diferentes e importantes empresas. Em 1992 foi publicado na Inglaterra o Relatório Cadbury, considerado o primeiro código de boas práticas de governança corporativa.
> No mesmo ano, foi divulgado o primeiro código de governança elaborado por uma empresa, a General Motors (GM) nos Estados Unidos. Sintomas do mesmo movimento são verificados pouco depois nos resultados de uma pesquisa realizada pelo fundo de pensão Calpers (California Public Employees Retirement System), nos Estados Unidos, que constatou que mais da metade das 300 maiores companhias daquele país já tinham sedus manuais de recomendações de governança corporativa.

Embora a proposta da governança corporativa seja louvável e envolta no marketing de desenvolvimento necessário e modernidade, é somente após os grandes escândalos de corrupção globais que as falhas no sistema de governança também são detectadas, forçando às companhias a criarem novos mecanismos de manutenção da governança corporativa. Noutros termos, a corrupção forçou às companhias a criarem a governança corporativa e a mesma corrupção apontou falhas nesse sistema gerencial de empresas.

Alguns desses escândalos são bem conhecidos, como a Enron, que em 2001 descobriram fraudes contábeis que inflacionavam resultados da empresa; a Pamalat, que tinha dívidas ocultas no montante de 14,3 bilhões de euros, escondidas por meio de falsificações das demonstrações financeiras, gerando um prejuízo no monte de 1% no PIB da Itália; os principais bancos de Wall Street, o Lehman Brothers e o Bear Sterns, que foram, respectivamente, a falência e vendidos a preços simbólicos porque se perderam nas complexas operações financeiras que faziam sem se atentarem nas supervisões de riscos pelos conselhos e no sistema de remunerações dos executivos (GODOI, 2020, *E-book*).

Porém, quando bem analisado, se percebe que a frente anticorrupção contra às práticas ilícitas praticadas por agentes públicos e privados remontam antes mesmo da década de 1990. Desde 1977, fruto de crimes de corrupção envolvendo autoridades de governos estrangeiros, já se tinham legislações chamadas de “anticorrupção”, como é o caso da *Foreign Corrupt Practice Act* (FCPA), promulgada com o objetivo (DEPARTMENT OF JUSTICE, *online*): [...] the purpose of making it unlawful for certain classes of persons and entities to make payments to foreign government officials to assist in obtaining or retaining business.

No plano internacional, agora sim a partir da década de 1990, também surgiram frentes legais contra à corrupção em diversos setores da sociedade. Entre elas está a Convenção Interamericana contra a Corrupção, de 1996, a qual, no seu preâmbulo, reconhece a corrupção como atentado a sociedade, a ordem moral e a justiça (OAS, *online*); a Convenção sobre o Combate da Corrupção de Funcionários Públicos Estrangeiros em Transações Comerciais Internacionais, de 1997, depois ratificada pelo Decreto Presidencial nº. 3.678, em 2000 (BRASIL, *online*); e a Convenção das Nações Unidas contra a Corrupção, de 2003, a qual colocou como uma das preocupações ao combate à corrupção o potencial desta para com (NAÇÕES UNIDAS, p. 4): [...] a estabilidade e a segurança das sociedades, ao enfraquecer as instituições e os valores da democracia, da ética e da justiça e ao comprometer o desenvolvimento sustentável e o Estado de Direito.

No Brasil, em 1994, foi promulgada a Lei nº 8.884/94, tratando sobre a transformação do Conselho Administrativo de Defesa Econômica (CADE) em Autarquia, com intuito de prevenir e reprimir às infrações contra a ordem econômica, principalmente no que dizia respeito a condutas anticoncorrenciais.

Porém, o avanço legal mais significativo no país ocorreu com a Lei nº 12.846/13, conhecida como Lei Anticorrupção (LAC). Juntamente com esta legislação, surgiu, em 2015, o Decreto 8.420/15, que regulamenta a LAC, trazendo parâmetros de como a Administração avaliará os programas de integridade nas empresas.

Como sequência natural a essa postura anticorrupção do mundo, oriunda, como já visto, dos grandes escândalos de corrupção, surge o compliance como alternativa para redirecionar a estrutura da governança corporativa para novos comportamentos compatíveis com a funcionalidade da empresa e a segurança dos investidores, como explica Coimbra e Manzi (2010, p. 2):

> No cenário mundial, casos como os atos terroristas nos Estados Unidos, em 2001, os escândalos de governança, como, por exemplo, os relacionamentos ao Banco Barings, Enrom, WorldCom e Parmalat e a mais recente crise financeira mundial, além da divulgação de casos de corrupção envolvendo autoridades públicas e também desvios de recursos em entidades do terceiro setor, acentuaram a necessidade de maior conformidade a padrões legais e éticos de conduta. O aumento da pobreza, dos problemas sociais, ambientais e, neste último caso, a chamada crise ambiental ampliou a abrangência do *compliance* para novos padrões desejáveis de comportamento. (Grifo original)

O compliance é uma palavra derivada do inglês *to comply* (CAMBRIDGE DICTIONARY, online), que significa, literalmente, cumprir, observar, executar o que foi imposto, o que pode ser convertido, conforme o contexto inserido, a medidas de cumprimento da lei. Esse não é um conceito que revela a complexidade desse programa e como ele é estruturado. Para ajudar a compreender a verdadeira natureza do compliance, Carvalho e Mendes (2017, e-book) delineiam:

> Um programa de compliance visa estabelecer mecanismos e procedimentos que tornem o cumprimento da legislação parte da cultura corporativa. Ele não pretende, no entanto, eliminar completamente a chance de ocorrência de um ilícito, mas sim minimizar as possibilidades de que ele ocorra, e criar ferramentas para que a empresa rapidamente identifique sua ocorrência e lide de forma mais adequada possível com o problema.

Na sua relação com a governança corporativa, o compliance poderia ser visto como meio de contribuição de efetividade da estrutura de governança. Esta,

por sua vez, para ter um bom desempenho precisa ter princípios básicos, como transparência, equidade, prestação de contas e responsabilidade corporativa, como explica o IBGC (2017, p. 4) na audiência pública que tratava sobre boas práticas de governança corporativa:

> O sistema de compliance deve ser entendido, portanto, como um conjunto de processos interdependentes que contribuem para a efetividade do sistema de governança e que permeiam a organização, norteando as iniciativas e as ações dos agentes de governança no desempenho de suas funções. Em sua base, devem estar os princípios básicos da boa governança corporativa – transparência, equidade, prestação de contas (*accountability*) e responsabilidade corporativa – apoiados, por sua vez, na prática constante da deliberação ética.

Na perspectiva prática, do dia a dia, o compliance, quando bem programado, possui um potencial notável de ajudar a empresa a chegar exatamente, ou bem perto, de onde queira. Olhando dessa forma, tal programa ganha ares de libertação frente aos problemas organizacionais deveras difíceis de se resolver no cotidiano laboral. Tratando sobre essa qualidade de vida empresarial, a Endeavor (2017, *online*), organização global sem fins lucrativos com objetivo de ajudar no empreendedorismo, vende o compliance para seu público sob o seguinte atrativo:

> É através das ferramentas de compliance que uma empresa pode alcançar com maior solidez seus objetivos estratégicos. Não estamos, portanto, falando de conceitos conflitantes. Ao contrário, a sinergia da empresa com todas as normas, ditames de regulamentação e controles internos eficientes, representam maior qualidade na atividade empresarial (respeito às normas de qualidade), economia de recursos (evitando gastos com multas, punições e cobranças judiciais) e fortalecimento da marca no mercado (empresa séria e ética).

Em contrapartida, no ambiente corporativo também surge uma expressão que merece destaque: “risco de compliance”. Tal expressão significaria risco legal, de sanções regulatórias, perdas financeiras ou de reputação, que pode afligir uma organização que esteja sofrendo falhas no cumprimento de leis, regulamentações, códigos de condutas e das boas práticas (COIMBRA e MANZI, 2020, *E-book*).

Embora esse termo “risco de compliance” pareça estar mais relacionada a incursão de medo às companhias que não fizerem o compliance, e, portanto, seria

uma forma de vender o programa em escalas cada vez mais alargadas, a bem da verdade é que foi só após a criação da Lei Anticorrupção que o compliance ganhou um novo significado, como alude Mendes e Carvalho (2017, e-book):

> Os efeitos da Lei Anticorrupção são reais e perceptíveis, extrapolando o debate meramente político-jurídico. Ainda que programas de compliance já existissem antes da Lei Anticorrupção, foi ela que deu a eles novo significado e impulsionou diversas áreas a se preocuparem com o tema. [...] O fortalecimento do combate à corrupção e a cartéis, em um círculo vicioso, levou a novas iniciativas do governo para conferir relevância ao tema – entre elas, destaca-se o Decreto 8.420/2015, que veio regulamentar a Lei Anticorrupção e, em matéria de compliance, trouxe parâmetros bastante detalhados sobre como tais programas serão avaliados pela Administração.

Para além de mero modismo, o compliance vem se tornando uma verdadeira tendência organizacional. Se em algum momento, mesmo conhecendo a proposta, algumas empresas se mostraram relutantes em reconhecerem o alinhamento do programa com a sociedade moderna, atualmente não enxergar essa tendência é estar alheio a realidade. Sobre essa nova perspectiva, explicam Coimbra e Manzi (2010, p. 19):

> Hoje, estar em *compliance* não é mais uma opção da empresa. As empresas estão sendo cada vez mais observadas e avaliadas pelo ponto de vista de seu comportamento como cidadãs. Como consequência, o *compliance* deve prevalecer em todo e qualquer passo da cadeira de valores. Além disso, experiências passadas demonstram que as atividades de *compliance* possuem uma valiosa proposta. Portanto, o *compliance* pode, agora, ser considerado e entendido como um modelo de negócio. (Grifos originais)

Parece que a tendência do compliance será trabalhar na acessibilidade do programa para empresas pequenas e de médio porte. Como se verá a seguir, nem todas as empresas estariam preparadas para a implementação do programa, e aquelas que estão esbarram no medo dos custos do investimento.

4.1 Os cuidados e desafios na implementação de um programa de compliance

No último levantamento de dinâmica demográfica do segmento formal das empresas brasileiras, em particular seus movimentos de entrada, saída e sobrevivência, realizado em 2015, o Instituto Brasileiro de Geografia e Estatística (IBGE) concluiu que 60% das empresas com média de 5 anos no mercado fecham, ou seja, em números, das 733,6 mil empresas abertas em 2010, somente 277,2 mil estavam operantes em 2015 (IBGE, *online*).

Em pesquisa realizada pela empresa de análise de crédito Serviço Central de Proteção ao Crédito Boa Vista (SCPCBOAVISTA, *online*), fazendo o mesmo levantamento que o IBGE, mas com datas mais atuais, se constatou o seguinte resultado:

Tabela 1 - Variações nas Falências e Recuperações Judiciais

	Set 2019/Set 2018	Set2019/Ago 2019	Acum. no ano	Acum. 12 meses
Pedidos de Falência	59,8%	-13,7%	1,8%	-1,7%
Falências Decretadas	16,5%	-34,7%	-6,5%	-6,0%
Pedidos de Recup. Jud.	38,5%	-29,9%	-17,4%	-12,0%
Recup. Jud. Deferidas	44,3%	-28,9%	-12,2%	-7,7%

Fonte: Boa Vista

Quando a mesma pesquisa se envereda para o balanço gráfico da distribuição das falências e recuperações judiciais por porte da empresa, se tem a seguinte realidade (*idem*):

Tabela 2 - Distribuição das falências e recuperações judiciais por porte

	Pequenas	Médias	Grandes
Pedidos de Falência	95,1%	3,8%	1,2%
Falências Decretadas	97,1%	2,6%	0,2%
Pedidos de Recuperação Judicial	92,5%	6,2%	1,3%
Recuperações Judiciais Deferidas	93,0%	5,8%	1,2%

Fonte: Boa Vista

Buscando descobrir os motivos da *causa mortis* das empresas, o Serviço Brasileiro de Apoio às Micro e Pequenas Empresas (SEBRAI) fez uma importante pesquisa no ano de 2014 e concluiu que os grandes problemas se concentravam em três categorias principais: o planejamento prévio, a gestão empresarial e o comportamento empreendedor (SEBRAI, 2014, p. 4). Em números, a pesquisa demonstrou, quanto aos empreendedores, que 46% não sabiam o número de

clientes que teriam e os hábitos de consumo, 38% não sabiam o número de concorrentes que teriam, 37% não sabiam a melhor localização, 33% não tinham informações sobre fornecedores, 32% não conheciam os aspectos legais do negócio, 31% não sabiam o investimento necessário para o negócio, 18% não levantaram a qualificação necessária da mão de obra, 61% não procuraram ajuda de pessoas ou instituições para abertura do negócio, 55% não planejaram como a empresa funcionaria em sua ausência, 55% não elaboraram um plano de negócios, 50% não definiram estratégia para evitar desperdícios, 50% não determinaram o valor do lucro pretendido, 42% não calcularam o nível de vendas para cobrir custos e gerar o lucro pretendido, 38% não identificaram necessidades atendidas pelo mercado, 24% não identificaram tarefas e os responsáveis por realiza-las e 21% não identificaram o público-alvo do negócio (*idem*, p. 6-7).

O mais curioso é que quando os empreendedores são questionados sobre o que seria mais importante para a sobrevivência da empresa, surgem as seguintes respostas (*idem*, p. 18):

Como se extrai dos dados levantados nessa pesquisa, os maiores problemas enfrentados pelas empresas estão relacionados com a falta de solidez nos objetivos e metas, o que faz delas estruturas frágeis ante as demandas comerciais. O mais curioso, como aponta o último gráfico, é que os gestores dos negócios sabem o que deve ser feito para conduzir a empresa no rumo correto,

mas por algum motivo não estão conseguindo desenvolver uma cultura de crescimento.

A princípio, esse cenário traçado em números revela que o ambiente comercial no Brasil é hostil, tanto pela notória burocracia conhecida, quanto pela falta de habilidades básicas dos gestores das empresas para as conduzirem ao sucesso.

Se por um lado esses dados podem desmotivar o setor empresarial, tendo em vista estarem entrando num ambiente com somente 40% de chances de sucesso, por outro, surge aqui uma grande e promissora oportunidade para o compliance.

É visando esse cenário fértil que estudos vem sendo feitos para descobrir o processo de estruturação da função e do programa de compliance na prevenção, detecção e monitoramento dos riscos, como é o caso do realizado pela KPMG sob título “Maturidade do Compliance no Brasil”, no qual alude a seguinte premissa (KPMG, 2015, p. 4):

> Diante desta perspectiva, o gerenciamento de riscos de ***compliance*** no Brasil vem passando por um processo de aprimoramento e de aumento de exigências em decorrência da dinâmica e da complexidade nos negócios, atrelado à frequente atualização e/ou emissão de novas leis e regulamentações, fortalecendo a necessidade de estruturar uma Função Eficiente de ***compliance*** para prevenir, detectar, monitorar e mitigar potenciais exposições a esses riscos. (Grifos originais).

Essa pesquisa da KPMG trouxe dados importantes para traçar o perfil de compliance das empresas que resolveram aderir ao programa (*idem*, p. 9):

> **46% das empresas respondentes classificaram a maturidade da estrutura e a função de *compliance* nos dois menores níveis de governança** considerados nesta pesquisa, sendo **12% “Sem Infraestrutura”** e **34% com “Infraestrutura Mínima”**. Algumas empresas entenderam possuir alguns pilares e componentes do compliance já mais bem estruturados. Aproximadamente, 19% definiram sua estrutura e sua função de ***compliance*** na “Função do Monitoramento”, enquanto 35% entendem que estão nos níveis mais elevados de maturidade, sendo 23% “Função de Integração” e apenas 12% “Alta Performance”. (Grifos originais).

Ainda que venha tendo uma boa adesão, existe uma espécie de fantasma intrínseco ao compliance quanto a acessibilidade de tal programa às empresas,

principalmente as de pequeno e médio porte. Talvez por ser vendido como novidade, e geralmente se ter como exemplo de implantação empresas de grande porte, criou-se uma imagem de algo vantajoso, mas longe da realidade prática. O Conselho Administrativo de Defesa Econômica (CADE) desmistifica essa visão, embora reconheça que a concorrência e os riscos estão intrínsecos ao porte da empresa e a sua individualidade (2016, p. 10-11):

> Organizações de todos os portes podem se beneficiar de um programa de compliance. No entanto, os riscos – principalmente de ordem concorrencial – a que uma organização está exposta variam de acordo com seu porte, posição de mercado, setor de atividades, objetivos, etc. Por esta razão, **não há um modelo único de programa de *compliance***. Cada programa deve respeitar as peculiaridades de cada indústria e ser revisto constantemente de modo a contemplar novos riscos que eventualmente possam surgir, como aqueles decorrentes de operações de fusões e aquisições, da introdução de um novo produto no mercado ou da entrada em um novo mercado geográfico com histórico de infrações em defesa da concorrência. (Grifos originais).

O *Department of Justice U.S.*, ao fazer um estudo sobre a evolução corporativa dos programas de compliance na realidade americana, entendeu, também, que a análise do programa de compliance deve respeitar a individualidade de cada caso (DEPARTMENT OF JUSTICE, 2020, *online*):

> Because a corporate compliance program must be evaluated in the specific context [...] We recognize that each company's risk profile and solutions to reduce its risks warrant particularized evaluation. Accordingly, we make an individualized determination in each case.

Essa questão da particularidade de cada programa para alcançar as especificidades de cada empresa realmente é um dos motivos da implantação do programa não ser tão barato e, ao mesmo tempo, ser tão complexo. Esse parece ser um problema difícil de superar, embora, segundo Carvalho e Mendes (2017, *E-book*), seja possível de fazê-lo:

> Se o compliance busca o cumprimento da lei, ainda que reconhecendo a impossibilidade de evitar completamente todo tipo de violação, e se é uma ferramenta que deixa nas mãos das organizações a atividade da fiscalização, é evidente que um programa de compliance depende, primordialmente, da estrutura particular de cada entidade.

> Em outras palavras, não há um modelo único ou receita de bolo para programas de compliance, e o desenvolvimento de um programa adequado depende do estudo profundo da estrutura da organização, da sua cultura corporativa, das legislações que se aplicam à sua atividade, entre outros. Consequentemente, o custo de implementação do compliance não é desprezível – ainda que seja plenamente possível que empresas de pequeno e médio porte, como como associações, sindicatos e outras entidades, adotem tais programas sem aportes elevados de capital.

Essa análise estrutural da empresa está presente nos programas de compliance como sendo uma das partes mais importantes. Não podia ser diferente, porque ao direcionar o programa para alcançar as especificidades de uma empresa, está se buscando, na verdade, encontrar sua personalidade, e a partir dela, com as limitações inerentes a cada organização, procurar o máximo de potencialidade em um curto, médio e longo prazo. Ao tratar da importância do estudo da estrutura da empresa que receberá o programa, Godoi (2020, *E-book*) aponta um quase passo-a-passo de como mapeá-la:

> Não existe uma fórmula única para a construção de um programa de integridade. Ele será sempre customizado, levando em conta os riscos, desafios, grau de maturidade, estratégia e limitações de cada organização. Ao estruturar um programa de compliance, a empresa deve mapear suas principais áreas de risco de descumprimento de leis, regulamentos estatais e políticas corporativas. Esses riscos variam de acordo com fatores internos e externos, como o setor de atuação da empresa, a legislação aplicável e suas atividades, as regiões geográficas em que atua, a estrutura de seu mercado, entre outros.

No entanto, há um elemento que deve estar presente em todas as empresas que busquem um programa de integridade: a cultura do compliance. A instalação desse ambiente corporativo envolto do compliance também é um desafio. Mobilizar uma estrutura corporativa para aderir um novo estilo de vida empresarial envolve muito mais que apenas vontade. O contexto para essa cultura, segundo Ducan (2017, *online*), embasada nas ideias de William C. Dudley, CEO do Federal Reserve Bank of New York, estaria numa era pós-financeira de maior regulamentação:

> In a post-financial crisis era of heightened regulation, increased regulatory enforcement, and renewed emphasis on corporate accountability, a recurring corporate governance theme has

> been the importance of corporate culture. As institutional investors continue to focus on long-term value creation, the impact of culture on the sustainable success of an organization is readily apparent. Corporations that neglect to build and maintain an ethical corporate culture that emphasizes compliance and transparency face greater risks than ever before.

Porém, para além de ser um projeto a longo prazo, a criação de uma cultura corporativa de compliance possui, também, objetivos práticos na constante evolução da empresa. Tratando sobre os pontos cegos que surgirão ao longo da vida empresarial, mesmo com compliance, Cueva e Frazão (2018, p. 100) explicam que sem a instalação eficiente dessa cultura corporativa não haverá a criação de um organismo vivo que constatando as falhas já agiria para corrigi-las:

> A instituição de uma cultura de compliance é particularmente importante, porque, tal como ocorre com o legislador, é impossível para a empresa prever de maneira exaustiva todos os riscos a que está sujeita e, principalmente, estipular, de maneira detalhada, a forma como devem comportar-se os agentes em toda e qualquer hipótese. Assim, embora seja importante estabelecer vedações expressas e claras, isso nem sempre será possível. Haverá sempre um campo de indefinições em que o comportamento adequado só poderá ser avaliado pelo agente na hipótese concreta. É aí que a cultura de obediência à legislação e a ética assume particular relevância.

Do ponto de vista prático, saber da necessidade de instalação de uma cultura de compliance no ambiente corporativo é bem diferente de vivê-la no dia-a-dia. Como já aludido nos parágrafos anteriores, modular toda uma estrutura de hábitos empresariais enraizados na mente dos funcionários por gerações não será tarefa das mais fáceis, principalmente no Brasil onde não há, notoriamente, um ambiente corporativo tão aquecido quanto os Estados Unidos da América, China e Europa. Somente com uma estratégia agressiva e repetitiva a empresa conseguirá instalar no ambiente corporativo o que seria o próximo do ideal de uma cultura de compliance. Com dicas práticas, o CADE (2016, p.20) aponta uma possível estratégia:

> Em grandes empresas, referências à política de compliance concorrencial pela alta direção em todos os eventos que reúnam funcionários, bem como veiculação, por meio de Cadeia interna de TV, de vídeos sobre o programa gravados pelo CEO e por Vice Presidentes (*sic*). Em empresas de menor porte, reforço

> sistemático da importância do programa para o sucesso dos empreendimentos.

Algumas empresas preferem adotar a postura de tensão na responsabilidade transferida como modelo de adesão ao código de conduta e, consequentemente, na criação de uma cultura de compliance. Uma dessas empresas é a Hospfar Indústria e Comércio de Produtos Hospitalares, que atua na distribuição de medicamentos e materiais de uso hospitalar. Na sua visão institucional, a meta é: Ser reconhecida pela indústria farmacêutica como a melhor parceira em distribuição de medicamentos e, pela sociedade, como uma empresa confiável e comprometida com a lei e com a ética (HOSPFAR, *online*). Para chegar nesse intento, contratou a criação de um programa voltado para suas especificidades, e na parte de adesão ao programa, mais especificamente nos itens 3 e 4, cobra o seguinte compromisso dos seus colaboradores (HOSPFAR, p. 28, *E-book*):

> 3. Todo colaborador deve ser informado sobre a existência do presente Código e, conforme suas responsabilidades, deve realizar sua leitura completa, assinando o respectivo certificado que, além de valer como prova de conhecimento, vale como declaração de concordância e de que não se encontra em situação de conflito com qualquer de suas disposições.
> 4. As normas de conduta estão sujeitas a revisões periódicas, sob a análise dos riscos relacionados às atividades da HOSPFAR, e todos os colaboradores devem fornecer subsídios para o aprimoramento dos mecanismos de integridade, inclusive apontando riscos que possam ter identificado.

Em consonância, não há como passar despercebido, também, que após o regulamento europeu de proteção de dados pessoais foi-se introduzida na dinâmica corporativa uma outra cultura, a de *accountability*, a qual permite às empresas demonstrarem suas observâncias das normas de proteção de dados pessoais e induz à adoção de programas de conformidade (CUEVA E FRAZÃO, 2018, p. 67).

Esse termo *accountability* é envolto no problema de tradução. Como explica Brito (2014, p. 55): [...] é um termo da língua inglesa, sem tradução exata para o português, que remete à obrigação de membros de um órgão administrativo ou representativo de prestar contas a instâncias controladoras ou a seus representados.

Numa visão geral, há autores que se satisfazem em traduzir referida palavra como sendo o dever dos agentes de governança em prestar contas de sua atuação, assumindo para si, e integralmente, as consequências de seus atos e omissões. (KUNHA e KALAY, 2019, p. 175).

Para outros autores, o termo não exprime todo o seu significado. Seria, na verdade, a responsabilidade dos agentes em explicar com regularidade o que estão fazendo, como estão, por que estão, quais os custos e quais os passos a seguir. Ou seja, na visão de Paiva (2009, p. 10), concluindo o raciocínio: Não se trata, portanto, apenas de prestar contas em termos quantitativos, mas de autoavaliar a obra feita, de dar a conhecer o que se conseguiu e de justificar aquilo em que se falhou.

De toda forma, essa cultura de *accountability* surge como resposta à necessidade de proteção efetiva das pessoas numa sociedade com mutação extraordinária, com múltiplos atores, nos quais a intervenção de um juiz *ex post* pode perder relevância e funcionalidade. Concluindo esse raciocínio, e indicando a estratégia que a regulamentação europeia adotou para forçar a introdução dessa cultura, Cueva e Frazão (2018, p. 67) aludem:

> Para dar credibilidade a essa nova abordagem, o regulamento prevê sanções pecuniárias que podem chegar a 4% do faturamento mundial da empresa, ficando claro que a proteção de dados pessoais deve ser levada a sério pelos atores públicos e privados, a partir do quotidiano operacional das organizações.

No entanto, a criação e implementação de um programa de compliance voltado também para a proteção de dados pessoais está entre as atividades de maior investimento, segundo pesquisa feita pelo *Ponemon Institute* (2011, p. 3, *E-book*), ao analisar os verdadeiros custos de implementação do compliance para empresas: Data protection and enforcement activities are the most costly compliance activities. In terms of the direct expense categories, data protection technologies and incident management top the list.

Explicando esses custos, e fazendo um balanço frente às organizações multinacionais que aderiram o referido programa, a pesquisa em comento detalha (*Idem*, p. 2):

> Multinational organizations in all industries must comply with privacy and data protection laws, regulations and policies designed to protect individuals' sensitive and confidential information. Compliance requires organizations to adopt and implement a variety of costly activities related to process, people and technologies. These activities include ensuring that they have professional staff dedicated to compliance as well as enabling technologies to curtail risk.

Em levantamento feito sobre o exame de fraudes no ambiente corporativo, e mais especificamente sobre a segurança na proteção dos dados dos clientes, Santos (2016, p. 22), em estudo junto a *Association of Certified Fraud Examiners*, apontou problemas relacionados com os próprios empregados na manutenção dos dados pessoais, mostrando, com isso, que até as atividades mais básicas precisam de uma atenção especial para a efetividade na proteção de tais dados:

> [...] a falta de conscientização entre os empregados de organizações que lidam com dados pessoais sobre o que exatamente constitui informações proprietárias, pode conduzir inevitavelmente à perda acidental das informações organizacionais. Os meios mais propícios de vazamento de informações são: a perda de computadores portáteis contendo informações privadas sem medidas de segurança como a proteção por senha ou criptografia de arquivos, descartar em lixeiras documentos importantes antes de destruir ou mesmo discutir informações confidenciais em lugares públicos onde pessoas alheias possam ouvir.

Esse cuidado com os dados pessoais de terceiros aumenta quando se está diante dos dados sensíveis desses terceiros. Como se viu, os dados sensíveis representam o mais íntimo que se pode coletar de um ser humano, motivo pelo qual os cuidados devem ser redobrados. Estruturar um programa de compliance voltado para proteção desses dados representa um desafio até na criação de um simples formulário de consentimento de utilização desses dados, pela complexidade já demonstrada até aqui.

A *International Labour Office - ILO*, na oportunidade da criação da *Protection of Worker's Personal Data*, fez menção importante quanto à responsabilidade dos profissionais da saúde no trato dos dados sensíveis (na época ainda não tinha essa nomenclatura) dos trabalhadores. Embora seja um documento voltado para a proteção de dados dos empregados, os princípios apresentados nele são bem atuais, estando alinhados com a exigência da nova

LGPD para com a proteção dos dados pessoais sensíveis no setor da saúde. Nesse sentido, se extrai dos itens 6.4, 6.5, 6.7 e 8.2, do referido documento (ILO, 1997, p. 3 e 4):

> 6.4. When an employer has obtained a worker's consent for the collection of personal data, the employer should ensure that any persons or organizations required by the employer to collect the data or conduct an investigation are at all times clear about the purpose of the inquiry and that they avoid all false or misleading representation.
> 6.5 (1) An employer should not collect personal data concerning a worker's: (a) sex life; (b) political, religious or other beliefs; (c) criminal convictions. (2) In exceptional circumstances, an employer may collect personal data concerning those in (1) above, if the data are directly relevant to an employment decision and in conformity with national legislation.
> 6.7. Medical personal data should not be collected except in conformity with national legislation, medical confidentiality and the general principles of occupational health and safety, and only as needed: (a) to determine whether the worker is fit for a particular employment; (b) to fulfil the requirements of occupational health and safety; and (c) to determine entitlement to, and to grant, social benefits.
> 8.2. Personal data covered by medical confidentiality should be stored only by personnel bound by rules on medical secrecy and should be maintained apart from all other personal data.

Como se vê, as responsabilidades e cuidados com o programa de compliance voltado para os dados pessoais sensíveis são muitos, embora não haja nenhuma garantia real de uma imunidade frente aos riscos de violação de tais dados. Realmente, como visto, medidas podem ser tomadas para potencializar a segurança dos dados, proteger os sistemas de manutenção dos dados, e, com isso, reduzir as chances de o programa falhar e fazer vítimas ao longo do caminho. Num ambiente onde os funcionários envolvidos no processo podem expor informações que deveriam ser confidenciais, o socorro que se busca é estruturar o programa de compliance seguinte fielmente pilares sólidos.

4.2 Os princípios de Caldicott como referencial na estruturação do programa de compliance

A partir dos requerimentos do *Federal Sentencing Guidelines*, foram criados os atualmente conhecidos "pilares" do compliance. Esse termo "pilares" foi um ajuste, já que o termo original são "componentes". De toda forma, mesmo

esses componentes/pilares, embora facilmente encontrados nos manuais de compliance, são iniciais e complexos, tendo que haver uma interação entre eles e outras temáticas. Nesse sentido, Serpa e Sibille (2016, *E-book*) explicam:

> Um Programa de Compliance é um sistema complexo e organizado, composto de diversos componentes, que interage com outros componentes de outros processos de negócios da empresa e, também, com outros temas. É um sistema que depende de uma estrutura múltipla que inclui pessoas, processo, sistemas eletrônicos, documentos, ações e ideias. A estes "componentes" dá-se o nome de "pilares" do programa de compliance.

Basicamente, tais pilares seriam, segundo Serpa e Sibille (2016, *E-book*): 1) Suporte da Alta Administração; 2) Avaliação de risco; 3) Código de Conduta e Políticas de Compliance; 4) Controles Interno; 5) Treinamento e Comunicação; 6) Canais de denúncia; 7) Investigações internas; 8) Due Diligence; 9) Monitoramento e Auditoria.

Esses pilares não são unanimes na sua divisão[28], o que prova ainda mais a complexidade da criação de um programa de compliance. Além de não serem unânimes, eles também não precisam necessariamente estar todos presente no referido programa, ficando a cargo dos responsáveis na criação do projeto a escolha dos pilares que se adequarão à realidade da empresa, como explica Giovanini (2014, p. 61):

> Quanto maior for a empresa, apresentará maior quantidade de atividades diferentes ou maior a complexidade de seus processos. Certamente, será mais complexa a implementação de um Programa de Compliance. [...] não há fórmula padrão para tal e, portanto, qualquer que seja a recomendação, faz-se necessária a customização para adequá-la a uma empresa [...] ficando a critério do leitor, suprimir as partes não aplicáveis a sua empresa.

Porém, parece haver um senso comum quanto a necessidade de iniciar a criação do programa pelo chamado *Compliance Risk Assessment* – CRA, ou, como é conhecido em português, pelo Mapeamento de Riscos de Compliance. Tal mapeamento, como sugestiona o próprio nome, ajuda na identificação e

---

[28] Para Geovanini (2014, p. 61), os componentes do programa de compliance seriam: 1) Identificação dos Risco; 2) Definição dos Requisitos; 3) Estruturação de um Projeto; 4) Desenho dos Processos e Controles; 5) Implementação dos Projetos e Controles; 6) Geração das Evidências; 7) Auditoria; 8) Ajustes; 9) Reteste.

formulação de medidas com intuito de diminuírem os riscos previamente mapeados. Segundo Bandarovsky (2018, *E-book*), em obra direcionada ao assunto:

> Compliance Risk Assessment (CRA) ou Mapeamento de Riscos de Compliance, é reconhecido mundialmente como um dos requisitos de validade e eficácia de um Programa de Compliance. É considerado também [...] como um dos processos mais complexos do Compliance Corporativo, gerando grandes preocupações e, até mesmo, chegando a tirar o sono de muitos de nós.

Nos Estados Unidos da América, em estudos voltados para legislação de práticas corruptas cometidos fora do solo americano mas de agentes sujeitos a sua jurisdição, o *Department of Justice* e a *Securities and Exchange Commission* foram responsáveis pela criação do documento intitulado *A Resource Guide to the U.S. Foreign Corrupt Practices Act*, no qual aponta, no seu *Chapter 5: Guiding Principles of Enforcement*, que trata das características básicas de um Programa de Compliance, a seguinte premissa sobre o *Risk Assessment* (DOJ e SEC, 2012, p. 58):

> Assessment of risk is fundamental to developing a strong compliance program, and is another factor DOJ and SEC evaluate when assessing a company's compliance program. One-size-fits-all compliance programs are generally ill-conceived and ineffective because resources inevitably are spread too thin, with too much focus on lowrisk markets and transactions to the detriment of high-risk areas.

.

No Reino Unido, o Mistério da Justiça, em 2011, embasado no artigo 9º da sua dura lei anticorrupção, intitulada "*United Kingdom Bribery Act*", publicou o documento chamado *Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing*. Nesse documento, mais precisamente na parte que elenca os seis princípios básicos para ajudarem organizações a se "blindarem" de corrupção, tem-se no princípio 3 o *Risk Assessment*, apresentado sob os seguintes argumentos (MINISTRY OF JUSTICE, 2011, p. 25):

> The commercial organisation assesses the nature and extent of its exposure to potential external and internal risks of bribery on its behalf by persons associated with it. The assessment is periodic,

> informed and documented. [...] The purpose of this principle is to promote the adoption of risk assessment procedures that are proportionate to the organisation's size and structure and to the nature, scale and location of its activities.

No Brasil, o Decreto nº 8.420/15, o qual, como já visto, regulamentou a Lei Anticorrupção, elencou, no seu inciso V, do artigo 18, que o fato de uma empresa possuir e aplicar um Programa de Integridade em consonância ao que está no Capítulo IV do mesmo decreto poderá possibilitar a redução de eventual pena de multa resultante da condenação em um Processo Administrativo de Responsabilização (PAR) nos percentuais de 1% a 4% do faturamento bruto da pessoa jurídica no exercício anterior ao da instauração do PAR. Com isso, nos termos do artigo 42, inciso V (Capítulo IV) do referido decreto, os parâmetros que serão utilizados para avaliar o Programa de Integridade serão: análise periódica de riscos para realizar adaptações necessárias ao programa de integridade.

Passada essa etapa de mapeamento de riscos, também seria de grande proveito para os programas de compliance, especialmente voltados para a proteção de dados pessoais sensíveis nas empresas do setor de saúde, se valerem dos chamados "Princípios de Caldicott" como um verdadeiro norte, principalmente na construção do código de ética e conduta do programa.

Já enraizados no Sistema de Nacional de Saúde inglês (NHS England), os Princípios de Caldicott foram criados em 1997, após um Painel de Revisão presidido por Dame Fiona Caldicott sobre como as informações dos pacientes eram tratadas em todo o Sistema Nacional de Saúde. Após a revisão, Caldicott estabeleceu seis princípios que as organizações deveriam seguir para garantirem que as informações que possibilitem a identificação de um paciente sejam protegidas e usadas somente quando for apropriado. Desde então, ao decidir se os agentes precisam usar informações que identifiquem um indivíduo, a organização deve usar os Princípios como teste de baliza (NHS, *online*).

Somente em 2000 os Princípio foram estendidos aos registros de assistência social de adultos, e em abril de 2013 Dame Fiona Caldicott na oportunidade da sua segunda revisão da governança da informação, em seu relatório *"Information: To Share Or Not To Share? The Information Governance Review",* informalmente conhecida como Revisão Caldicott2, introduziu um novo 7º princípio de Caldicott. (*idem*).

Apresentando tais princípios, tem-se no Princípio 1 o seguinte texto: *Justify the purpose(s) for using confidential information*. Segundo este, todo uso ou transferência de dados pessoais sensíveis dentro de uma organização devem ser claramente justificados, examinados e documentados, com os usos contínuos revisados regularmente, por um agente responsável (*idem*).

O Princípio 2 alude: *Don't use personal confidential data unless it is absolutely necessaryl*. Os dados pessoais sensíveis não devem ser incluídos no sistema de armazenamento, a menos que sejam essenciais para o(s) objetivo(s) especificado(s) para tal manutenção. Ou seja, noutros termos, a necessidade de identificação dos pacientes deve ser considerada em cada estágio de satisfação do(s) objetivo(s) (*idem*).

No Princípio 3, tem-se: *Use the minimum necessary personal confidential data.* Quando o uso de dados pessoais sensíveis é considerado essencial, a inclusão de cada item individual desses dados deve ser especificada e justificada para que a quantidade mínima de dados pessoais confidenciais seja transferida ou acessível, conforme necessário para que uma determinada função seja executada (*idem*).

No Princípio 4 está escrito: *Access to personal confidential data should be on a strict need-to-know basis*. Somente as pessoas que precisam acessar dados pessoais sensíveis devem ter acesso a eles e esse acesso deve ser restrito apenas aos itens de dados que precisam ver. Isso pode significar a introdução de controles de acesso ou a divisão de fluxos de dados em que um fluxo de dados é usado para vários propósitos. (*idem*).

Nos termos do Princípio 5: *Everyone with access to personal confidential data should be aware of their responsibilities*. Aqui se alude que devem ser tomadas medidas para garantir que aqueles que lidam com dados pessoais sensíveis - tanto a equipe clínica quanto a não clínica - sejam conscientizados de suas responsabilidades e obrigações de respeitar a confidencialidade do paciente. (*idem*).

O Princípio 6 é direto: *Comply with the law*. Todo uso de dados confidenciais pessoais deve ter respaldo legal. O agente que manipula dados pessoais sensíveis deve ser responsável por garantir que a organização cumpra os requisitos legais (*idem*).

Por fim, o Princípio 7 aduz: *The duty to share information can be as important as the duty to protect patient confidentiality*. Os profissionais de saúde e assistência social devem ter confiança para compartilhar informações no melhor interesse de seus pacientes, dentro da estrutura estabelecida por esses princípios. Eles devem ser apoiados pelas políticas de seus empregadores, reguladores e órgãos profissionais (*idem*).

Não é difícil perceber que esses princípios são verdadeiras balizas para um programa de compliance voltado, como já dito, para área da proteção de dados sensíveis no setor da saúde. Na Inglaterra, esses princípios viraram o próprio "compliance", de modo que para resguardá-los se criou a figura do *Caldicott Guardian*, regulados, em parte, pelo órgão nacional chamado de *The United Kingdom Caldicott Guardian Council* (UKCGC, *online*):

> A Caldicott Guardian is a senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly.
> All NHS organisations and local authorities which provide social services must have a Caldicott Guardian.
> The Council is not a professional body and does not have responsibility for regulating Caldicott Guardian activities. It is therefore unable to assist with enquiries related to the conduct of individual Caldicott Guardians.

Porém, uma pergunta que pode surgir é o que seria de fato essas informações pessoais do paciente, dentro do alcance dos Princípios de Caldicott? Essa resposta já foi dada no documento intitulado "*Confidentiality: NHS Code of Practice*", afirmando o seguinte (NHS, 2003, p.7):

> A duty of confidence arises when one person discloses information to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence. It – a. is a legal obligation that is derived from case law; b. is a requirement established within professional codes of conduct; and c. must be included within NHS employment contracts as a specific requirement linked to disciplinary procedures.

Vale destacar o cuidado que o *Caldicott Guardian* precisa ter não só com a confidencialidade dos dados pessoais sensíveis colocada sob os seus cuidados, mas também no alinhamento do tratamento desses dados com o programa de integridade. No documento intitulado "*A Manual for Caldicott Guardians*", nas

responsabilidades 18, 19 e 20, fica claro as diligências que o referido profissional deverá fazer (UK Caldicott Guardian Council, 2017, p. 5 e 7):

> 18. Confidentiality & data protection expertise: the Caldicott Guardian should develop a strong knowledge of confidentiality and data protection matters, drawing upon support staff working within the organisation's Caldicott and information governance functions, but also on external sources of advice and guidance where available.
> 19. Internal information processing: the Caldicott Guardian should ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff. The key areas of work that need to be addressed by the organisation's Caldicott function are detailed in the Information Governance Toolkit.
> 20. Information sharing: the Caldicott Guardian should oversee all arrangements, protocols and procedures where confidential personal information may be shared with external bodies and others with responsibilities for social care and safeguarding. This includes flows of information to and from partner agencies, sharing through IT systems, disclosure for research, and disclosure to the police.

Porém, como apontam Graham e Greenough (2004, p. 246), a questão da confiabilidade dos dados pessoais sensíveis está para além de mero protocolo de armazenamento de dados em algum sistema, envolve mesmo a própria relação entre médico e paciente, motivo pelo qual deve-se chamar a atenção dos profissionais e escolas médicas quanto a seriedade dessas informações:

> Confidentiality is central to the trust between patients and doctors. All patient information is confidential and must be protected and used appropriately by all members of the healthcare team. This applies not only to clinicians, but also to undergraduate and postgraduate students working in clinical areas and to those undertaking research. Trusts are responsible for ensuring that all their staff are aware of the issues around data protection and confidentiality. The onus rests with medical schools to ensure confidentiality issues are taught and that students have understood their implications

Na visão de Aljareh, Dobson e Rossiter (2003, *online*), os requisitos indispensáveis que deverão estar presentes em qualquer atuação de controle dos dados confidenciais (referência a dados pessoais sensíveis, na LGPD) do paciente se resumiriam nos cinco seguintes:

> With respect to the patient's rights, recente legalisations and publication in the field support five important aspects:
> 1. Patient oriented approach: an item of information about a patient should be owned by the patient described by the information. 2. Privacy: patient privacy should be maintained to a high standard as a result of fair and lawful use of the patient's confidential information. 3. Transparency: the patient should be made aware of all the use made of his information. 4. Public interest: the need of the community may override the need of individuals in some exceptional cases. 5. Legal requirements: a trial case may require disclosure of a patient's confidential information. However this should be very restricted and limited by the case after detailed explanations of why the information disclosure is essential.

No Brasil, os referidos princípios receberam uma atenção pelo Conselho Federal de Medicina. Ao disciplinar a telemedicina como forma de prestação de serviços médicos mediados por tecnologias, na Resolução CFM nº 2.227/2018, o Conselho Federal, nas suas considerações iniciais, fez a seguinte alusão (CFM, *online*):

> **CONSIDERANDO** que o registro digital para atuar por telemedicina deve ser obrigatório e confidencial nos termos das leis vigentes e dos Princípios de Caldicott (2013), do National Health Service (NHS), que definem:
> I - que seu uso deve ser necessário, justificado e restrito àqueles que deles precisem;
> II - que todos aqueles que os utilizem devem ser identificados, estar conscientes de sua responsabilidade e se comprometer tanto a compartilhar como a proteger os dados e informações a que tiverem acesso e forem colocados à disposição dos médicos ou anotados em Sistemas de Registro Eletrônico/Digital de Saúde; (Grifo original).

Se está claro que os Princípios de Caldicott estão firmados e funcionando, inclusive já se estendendo até para o Brasil, o trabalho agora seria alocá-los no projeto real de um programa de compliance no Brasil.

Tomando como referência os pilares apresentados por Serpa e Sibille, após a avaliação de risco, e a criação do Mapa de Risco, o próximo passo na criação de um Programa de Compliance seria o Código de Conduta e de Ética, pilar este que acreditamos ser o ambiente apropriado para incluir os aludidos princípios.

Embora estes dois códigos estejam presentes num único pilar (e geralmente num único documento), a realidade é que guardam significados e propostas distintas (CUEVA e FRAZÃO, 2018, p. 97):

> O Código de Ética nada mais é do que um documento escrito, no qual serão estabelecidos os valores e princípios que devem ser observados por todos os funcionários, os administradores e os terceiros que se relacionam com a empresa. Além do Código de Ética, pode haver também um Código de Conduta, que especifique, de maneira mais detalhada, as condutas vedadas e autorizadas e fixe deveres concretos aos colaboradores. Frequentemente, o Código de Ética e Conduta integram um único documento.

No entanto, não se pode perder de vista o objetivo principal de tais códigos, o qual vai além de mera prática comportamental dos agentes internos. Ajudando nessa compreensão expandida, Cueva e Frazão (2018, p. 98) explicam:

> O objetivo principal do(s) Código(s) é, antes de tudo, deixar claro para todos os administradores e funcionários, assim como para terceiros, que a empresa se preocupa com a observância da legislação e que pretende instituir uma cultura organizacional baseada na ética e no cumprimento legal. [...] cumprem também a importante função de traduzir, em palavras mais simples e de fácil compreensão, os diversos deveres legalmente exigíveis tanto da empresa como das pessoas naturais que dela fazem parte.

Nos EUA, o Código de Conduta é tido como primeiro passo para as empresas estruturarem um programa de compliance que vise ser anticorrupção. No já destacado documento intitulado "*A Resource Guide to the FCPA U.S. Foreign Corrupt Practices Act*" há um levantamento interessante sobre a importância do referido código (DOJ e SEC, 2012, p. 57):

> The company's code of conduct is often the foundation upon which an effective compliance program is built. At DOJ has repeatedly noted in its charging documents, the most effective codes are clear, concise, and accessible to all employees and to those conducting business on the company's behalf.

O conteúdo básico desses Códigos, para que surtam o efeito e alcance almejados, deverá ser imparcial, justo, ausente de preconceitos e ambiguidades, com linguagem apropriada aos públicos de destino e aplicável a todas as pessoas, sem distinção e discriminação (GIOVANINI, 2014, p. 136)

Um exemplo muito bom de um Código de Conduta com essa proposta de ser claro e conciso, como orientou o documento acima, e seguindo as características básicas apontadas pelo último autor citado, é o da empresa Novartis. Esta empresa é do ramo de produção e distribuição de medicamentos, e como tal precisa ter acesso a dados pessoais sensíveis dos seus consumidores para ajustar a sua produção e desenvolver suas pesquisas. Como forma de se alinhar à nova LGPD, criou a seguinte conduta sobre a privacidade dos referidos dados (2018, p.7):

> Respeitamos os direitos de privacidade de todos os públicos com os quais nos relacionamos; como nossos associados, pacientes, médicos, acionistas e outros. Informamos as pessoas sobre a coleta e o processamento de seus dados pessoais, permitindo-lhes tomar decisões informadas e exercer seus direitos. Recolhemos e processamos dados pessoais somente para efeitos de negócios específicos e legítimos e protegemos esses dados contra acessos não autorizados.

No entanto, como até já tratado mais acima na questão da criação da cultura de compliance, implantar de forma eficaz um Código de Ética ou de Conduta numa empresa exigirá um plano de ação nas suas áreas de relacionamentos. Para obter sucesso, esses códigos deverão ser devidamente e massivamente comunicados e explicados, sem deixar dúvidas de suas aplicações em aberto (GIOVANINI, 2014, p. 136).

Fazendo a mesma leitura estratégica, o Instituto Ethos, na oportunidade da criação do seu guia de reflexões e sugestões na formulação e implantação do Código de Ética nas empresas, aludiu (2000, p. 16):

> Portanto, para ser bem sucedido na implantação de um Código de Ética é necessário desencadear um conjunto de ações concretas, relacionadas ao mais difícil de todos os terrenos: o comportamento das pessoas. Pois as empresas não pensam, decidem, agem, determinam ou obedecem. Quem faz tudo isso são seus integrantes, por meio da qualidade de seus múltiplos relacionamentos. O CE de uma empresa só ganha materialidade nas ações das pessoas relacionadas à empresa.

Na posse de todas essas informações, às empresas voltadas para a criação de programa de compliance com foco na nova LGPD, e mais especificamente na proteção de dados pessoais sensíveis do setor de saúde,

parecem estar munidas com a benção de ter predecessores que há alguns anos já estruturaram verdadeiras diretrizes no tratamento de tais dados e, ainda, ofereceram os mecanismos necessários para fazê-los serem aplicados e cumpridos.

Sem dúvida, as empresas que lidam com os referidos dados pessoais poderão enxergar com boas perspectivas os seus ajustes à nova Lei Geral de Proteção de Dados.

4.3 O formulário de consentimento como ferramenta na abordagem inicial para com o detentor dos dados pessoais sensíveis

Embora a LGPD venha repleta de mudanças estruturais na lida com os dados pessoais de terceiros, sem dúvida o ponto chave poderia ser considerado a questão do consentimento do detentor dos referidos dados.

Essa questão é de fundamental importância principalmente quando não se perde o foco da proposta das legislações de proteção de dados pessoais: a tentativa de blindagem do uso indevido ou manipulado dos dados pessoais de usuários de programas e serviços ofertados por quem não recebeu autorização para fazer o tratamento desses dados.

É uma nova postura que empodera o consumidor, lhe dando uma sensação de segurança e controle sobre sua vida privada. Fazendo essa mesma leitura, a Serpro (*online*), orientando sobre a nova tendência, afirma:

> É o titular, ou seja, a pessoa a quem se referem os dados que deve, se quiser - ao ser questionada, de forma explícita e inequívoca - autorizar que suas informações sejam usadas, por empresas e órgãos públicos, na hora da oferta de produtos e serviços, gratuitos ou não.
> Portanto, com a nova lei, fica claro que quem é o verdadeiro dono do dado não é aquele que o utiliza, nem aquele que o salvaguarda em bancos de dados. Nada disso, o dado pessoal é estritamente da pessoa a quem ele diz respeito. Na teoria isso parece algo óbvio, mas na prática não é bem assim. E tem muito dado particular sendo usado para fins que seu dono ou dona real sequer sabem. Usos, inclusive, que podem até mesmo prejudicá-los.

Ainda que o termo “consentimento” esteja esparso na LGPD, parece que o legislador antecipou algumas questões pertinentes que surgiriam nos debates jurídicos, fazendo da própria lei uma boa fonte de consulta.

Nos termos do art. 5º, inciso XII, da referida lei, o conceito de consentimento é: [...] manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

A Diretiva 95/46/EC – *European Commission* (EDPB, *online*), que tratava sobre a proteção das pessoas em relação ao tratamento de dados pessoais e sobre a livre circulação desses dados, já afirmava, no seu art. 2º, item H, que o consentimento do titular seria: shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

Embora sejam um ponto de partida interessante, referidos conceitos são mais enxutos (não incompletos) do que o apresentado pelo Regulação Geral da União Europeia, a qual, no seu artigo 4º, item 11 (GDPR, *online*), assim aponta:

> (11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Porém, essa série de requisitos apresentam alguns desafios práticos que devem ser dirimidos de forma cuidadosa pela administração da empresa. Por isso, não bastarão medidas gerais, como bem alude Murino (2018, *online*):

> Muitas vezes, entretanto, a mera atualização de Termos de Uso e Políticas de Privacidade não é suficiente para garantir sua eficácia e adequação às supracitadas leis de proteção de dados. Deve-se atentar para aspectos práticos, que, se não implementados corretamente, podem vir a invalidar referidos documentos, deixando as empresas desprotegidas em caso de eventual disputa.

Ao analisar os requisitos iniciais impostos no art. 5º da LGPD, pode-se começar pela manifestação livre. Na visão de Murino (2018, *online*):

> Para que o consentimento seja considerado livre, deve ser conferido ao usuário pleno controle sobre o tratamento de seus dados pessoais. O usuário deve poder escolher quais dados fornecer, quais dados não fornecer, e deve poder retirar seu consentimento a qualquer momento.
> Em outras palavras, não pode o usuário ser compelido a consentir com o tratamento de seus dados pessoais para ter acesso a

> determinada aplicação de internet. Nesse caso, o consentimento do usuário não é considerado livremente fornecido, podendo o contrato ser invalidado por ineficácia da aceitação.

Na oportunidade da criação do documento intitulado "*Guidelines 05/2020 on consent under Regulation 2016/679*", endossado pelo Conselho Europeu de Proteção de Dados, tratando, entre outras coisas, sobre a necessidade de mais esclarecimentos sobre a questão da validade do consentimento fornecido pelo titular dos dados ao interagir com o chamado "*cookie walls*", foi explicado o significado de *freely given* (EDPB, 2020, p. 5) da seguinte forma:

> The element "free" implies real choice and control for data subjects. As a general rule, the GDPR prescribes that if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid. If consent is bundled up as a non-negotiable part of terms and conditions it is presumed not to have been freely given. [...] The notion of imbalance between the controller and the data subject is also taken into consideration by the GDPR.

Essa nova postura de consentimento livre irá impedir, também, que manobras cínicas sejam ofertadas ao consumidor, como aqueles casos clássicos onde para se fazer uso de determinado produto ou serviço o consumidor tem que fornecer acesso aos seus dados pessoais, como bem desenha o exemplo dado no documento acima intitulado (*idem*, p. 6):

> A mobile app for photo editing asks its users to have their GPS localisation activated for the use of its services. The app also tells its users it will use the collected data for behavioural advertising purposes. Neither geolocalisation or online behavioural advertising are necessary for the provision of the photo editing service and go beyond the delivery of the core service provided. Since users cannot use the app without consenting to these purposes, the consent cannot be considered as being freely given.

Em síntese, só será exigido o consentimento como condição para usufruto de determinado produto ou serviço nos casos onde o tratamento de dados for necessário para se conseguir prestar aquele serviço ou usar aquele produto. Caso contrário, se porventura as exigências cobradas do consumidor forem para além do necessário para uso do serviço ou produto, tal consentimento não será livre.

O segundo requisito que merece destaque é o consentimento informado. Segundo o Recital 42, da GDPR: For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended.

Ao fazer a sua ponderação sobre o consentimento de tratamento de seus dados pessoais, o consumidor precisa ter a sua disposição informações suficientes sobre a empresa solicitante, os serviços ou produtos ofertados e qual o grau de segurança e confidencialidade do tratamento de seus dados. Só com isso o possuidor dos dados poderá fazer uma análise mais racional sobre o que está aderindo e/ou autorizando, como alude Soares (2019, *online*):

> Nesse sentido, produtos e serviços que intencionem coletar dados pessoais devem se adequar a esse quadro normativo, embutindo em seus sistemas soluções que assegurem ao titular dos dados a possibilidade de manifestar seu consentimento de maneira informada. A proteção à privacidade deve, portanto, estar integrada, *by design* e *by default*, aos ditos produtos e serviços, seguindo a orientação da GDPR, que tanto inspirou a LGPD. Os agentes de tratamento de dados que pretendam se valer do consentimento dos titulares devem, assim, oferecer aos titulares dos dados pessoais um ambiente neutro, transparente e acessível, no qual o consentimento possa ser tomado livremente e de maneira informada. (Grifos originais).

Sem esses cuidados, segundo o documento *Guidelines 05/2020* (*idem*, p. 15), o controle junto ao usuário será mera ilusão, não tendo validade para o tratamento dos dados, haja vista o art. 5 da GDPR reforçar a necessidade do consentimento informado, uma vez que representaria um princípio de transparência intimamente relacionado aos princípios da justiça e legalidade.

O último requisito do consentimento exigido pela LGPD é o inequívoco, o qual, nas palavras de Murino (2018, *online*):

> [...] depende de manifestação por meio de um ato positivo do usuário. Em outras palavras, deve haver uma ação do usuário indicando sua aceitação, seja pelo envio de um e-mail, assinatura eletrônica, ou até mesmo por um clique em local determinado.
> A aceitação não pode ser passiva, de forma que o silêncio do usuário não pode ser considerado consentimento.

Terminando também com sua série de conceituações, aquele mesmo documento, o *Guidelines 05/2020*, ao tratar do consentimento inequívoco

(chamado na legislação europeia de *unambiguous indication of wishes*) (*idem*, p. 18) declarou as seguintes premissas:

> The GDPR is clear that consent requires a statement from the data subject or a clear affirmative act, which means that it must always be given through an active motion or declaration. It must be obvious that the data subject has consented to the particular processing. [...] A “clear affirmative act” means that the data subject must have taken a deliberate action to consente to the particular processing. Recital 32 sets out additional guidance on this. Consent can be collected through a written or (a recorded) oral statement, including by electronic means. [...] Silence or inactivity on the part of the data subject, as well as merely proceeding with a service cannot be regarded as an active indication of choice.

Assim como fez no primeiro requisito, o referido documento aponta um exemplo casual muito elucidativo (*idem*), mas que dessa vez seria considerada uma prática válida junto ao consumidor:

> When installing software, the application asks the data subject for consent to use non- anonymised crash reports to improve the software. A layered privacy notice providing the necessary information accompanies the request for consent. By actively ticking the optional box stating, “I consent”, the user is able to validly perform a ´clear affirmative act´ to consent to the processing.

Além de tudo isso, no final do texto legal aludido da LGPD há a expressão “para uma finalidade determinada”, se referindo ao tratamento de dados munido daqueles três requisitos apresentados. Porém, para que o usuário titular dos dados possa compreender a dimensão dos direitos que está ofertando aos cuidados de terceiros, necessário se faz detalhar aqueles três requisitos ao nível elementar de comunicação, como deixa transparecer as palavras de Soares (2019, *online*):

> Neste particular, não parece suficiente meramente comunicar ao titular que seus dados poderão ser coletados. Cabe ao controlador ou operador informar a forma, duração e finalidade do tratamento dos dados, as suas responsabilidades, os riscos a ser suportados pelo titular, bem como a maneira de revogar autorizações anteriormente concedidas, de maneira transparente. Ao assim fazer, o titular terá condições de optar, ou não, por determinado produto ou serviço que colete dados, podendo, inclusive, manifestar consentimento específico para determinado tipo de

> tratamento e não para os outros visados pelo controlador ou operador, além de revogar tal consentimento a qualquer momento.

Seguindo o desenvolvimento legal da própria LGPD, percebe-se um alinhamento de dispositivos legais que deixa claro as etapas corretas da verificação do consentimento do usuário conforme intenção originária do legislador (BRASIL, *online*):

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> [...]
> Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.
> [...]
> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
> § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

No entanto, antes de tratar dos maiores cuidados que os agentes de tratamento deverão ter para com a manipulação dos dados, é precisa saber também que, conforme já superficialmente tratado acima, há dados de saúdem que podem ser tratados sem consentimento do titular[29], haja vista ainda vigorar outras normas que estabelecem responsabilidades para aqueles que comercializam produtos voltado para saúde ou prestam serviços de saúde (GIRÃO, 2020, *online*).

Esses cuidados com o consentimento aumentam na área da saúde, uma vez que a LGPD, como já exaustivamente tratado, considera os dados relativos à

[29] Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: [...] II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

saúde como sensíveis (art. 5º, II), ou seja, dados pessoais que guardam um potencial lesivo muito grande à intimidade e vida privada do paciente/consumidor, o que justificaria tratar o consentimento com maior critério dos artigos citados acima. Mais ainda quando se lida com os dados de crianças e adolescentes, onde o tratamento de dados, nos termos parágrafo 1º, do art. 14, da LGPD, deverá ser realizado: [...] com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

No entanto, não há como deixar de notar o cuidado da nova legislação com o tratamento de dados pessoais especificamente para a tutela da saúde em si, oportunidade que dispensará o consentimento em prol de cuidados maiores, como aponta Girão (2020, *online*):

> A LGPD também estabeleceu como base legal o tratamento de dados pessoais para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (art. 7º, inciso VIII e art. 11, II, "f"). Ou seja, nessa primeira análise, os profissionais de saúde (médicos e terapeutas, de um modo geral), hospitais, clínicas, centros de diagnóstico, devem prestar assistência à saúde e, por questão ética, zelar pela privacidade e intimidade dos pacientes. Portanto, independentemente de consentimento, devem cuidar para que os dados pessoais sejam tratados EXCLUSIVAMENTE para os fins terapêuticos, de diagnóstico, enfim, para a garantia do atendimento à saúde. (Grifo original).

Diante desse contexto, e dentro da proposta do trabalho, acreditamos que uma boa ferramenta de abordagem para coleta de dados pessoais sensíveis de pacientes que dão entradas em hospitais e clínicas seria em forma de um formulário de consentimento, o qual deveria deixar claro para o usuário dos dados sensíveis todos aqueles três requisitos já tratados numa linguagem simples e acessível, e dispondo de opções de escolha que deixassem o consumidor no controle da disposição de seus dados, não se limitando, tão somente, à deixar como opção um "não" ou "sim".

Talvez o maior problema seja o momento de coleta de tais dados. Como é notório, hospitais, principalmente, nem sempre são locais calmos. É normal nesses ambientes a chegada de urgências, e a coleta das informações do paciente poderá ser prejudicada, como explica Girão (2020, *online*):

> Para ilustrar, imagine um paciente chegando ao pronto socorro do hospital para tratar um cálculo renal (pedra nos rins). Não se sabe qual o desdobramento do atendimento. Mas antes de iniciar seu atendimento, imagine se fosse necessário coletar dele consentimento para que os dados coletados pelo hospital (controlador) possam ser compartilhados com o centro de diagnósticos (terceirizado, normalmente), médicos e enfermeiros que o atenderão (operadores dos dados). Dificilmente ele concederá o consentimento informado, ele quer é o atendimento!

Esse poderia ser um ponto de embate legal entre a necessidade do consentimento e a situação factual que o programador do programa de compliance voltado para essa área deveria enfrentar. Porém, e aqui há de se dar os créditos ao legislador, nas situações onde se percebe a vulnerabilidade factual do titular dos dados, como é o caso acima, o parágrafo 4º, do art. 11, da LGPD, criou uma proteção especial, tanto para o titular, quanto para a empresa do setor de saúde, ao dispor o seguinte:

> § 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados.

Nesse ensejo, com os cuidados do não uso dos dados sensíveis para vantagem econômica, mas tão somente para ter o suficiente para controle operacional do próprio hospital e em benefício do paciente, o consentimento estará implícito, embora a uso limitado de dados.

Outro aviso importante que deverá constar no formulário de consentimento disposto ao titular dos dados sensíveis, o que acabará criando ainda mais aquele sentimento de controle sobre os dados pelo paciente, é a possibilidade do consentimento ser revogado a qualquer momento, como deixa claro o parágrafo 5º, do art. 8º, da LGPD, mediante: [...] manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação [...].

Com esses cuidados aqui apresentados, acreditamos que o formulário de consentimento se reveste como uma ferramenta integrativa ao programa de

compliance suficiente para suprir não só a parte técnica das exigências legais, mas, também, o *animus* em trazer para o controle dos dados o próprio titular, gerando no paciente/consumidor um sentimento muito importante de justiça, transparência e respeito à sua intimidade e vida privada.

5 CONSIDERAÇÕES FINAIS

A economia nunca foi estática e sempre seguiu o percurso de constante desenvolvimento com novas tendências. Confirmando essa premissa, atualmente o mercado de dados pessoais virou campo de disputa econômica de verdadeiras multinacionais.

O mundo está vivendo uma nova fase civilizacional envolvendo o ambiente virtual, e para se alinharem a essa nova realidade, as empresas precisarão se adaptar à tecnologia de aquisição, processamento e uso final de dados pessoais, principalmente após a criação de regulamentações sobre o uso desse tipo de dados em todo o mundo.

Como se viu no primeiro capítulo, por trás das iscas tecnológicas em forma de aplicativos ou serviços voltados para o prazer, ou até praticidade, há um verdadeiro mercado de negociações de dados pessoais deixados pelos consumidores constantemente no dia-a-dia.

Até o ano de 2018, antes da nova Lei Geral de Proteção de Dados Pessoais ser criada, a sensação que se tinha era da existência de um mercado clandestino de comercialização de dados pessoais, principalmente porque os consumidores não tinham conhecimento dos fins de uso daqueles dados fornecidos gratuitamente, mantendo a ingenuidade que referidos dados se limitavam a ficar em servidores para fins inocentes, sem imaginar que esses mesmo dados estavam sendo cruzados para traçar perfis que faziam com que a máquina lhe conhecesse mais do que pessoas próximas.

Ante esse cenário onde o uso dos dados pessoais começou a apontar como um negócio de grande potencial econômico, e ao mesmo tempo com grande poder de lesividade à intimidade e vida privada do titular consumidor, surge uma preocupação evidente em regular o comportamento daquelas empresas pelo que se convencionou chamar pelas legislações da União Europeia e do Brasil de “tratamento de dados”, de modo a gerar um possível controle sobre quem lidava com dados pessoais de terceiros e como o faria, ficando este critério sobre os cuidados de condicionamento legal.

Essa medida legal não fez com que o fluxo de venda dos dados pessoais tenha diminuído (até porque a lei só entrará em vigor em 2021), embora se espere uma diminuição, principalmente por parte de empresas que atuavam nesse

mercado de forma clandestina e inconsequente. Porém, para as empresas sérias, que precisam lidar com dados pessoais de terceiros para melhorarem seus serviços e produtos, a nova lei regulamentadora trará alguns bons desafios a serem vencidos.

Como visto no segundo capítulo, a intenção da nova lei não é criar tão somente mudanças pontuais, mas reconfigurar totalmente a estrutura das empresas para o tratamento de dados pessoais de terceiros. Essa estrutura virá tanto em forma de diretrizes legais, quanto no olhar atento da Autoridade Nacional de Proteção de Dados (ANPD), sob a coação de multa de até cinquenta milhões de reais para os infratores.

É inegável que tais mudanças, com multas que podem literalmente levar uma empresa a falência, causam incômodo no ambiente do mercado. No entanto, não há muito tempo para reclamações, e sim reunir forças e estratégias para se sobressair nesse novo cenário, principalmente para as empresas do setor de saúde, as quais além de terem que lidar obrigatoriamente com dados pessoais de seus pacientes, a maioria desses dados são os chamados “sensíveis”.

Lidar com os dados sensíveis guarda um desafio à parte. Primeiro porque existe um tratamento específico para os referidos dados, ficando ainda mais engenhoso se forem dados sensíveis de crianças e adolescentes. Segundo que cada um dos dados sensíveis guarda em si próprio um potencial lesivo aos direitos fundamentais do usuário/paciente, aumentando em muito a responsabilidade das empresas do setor de saúde para fazerem o devido tratamento de tais dados, principalmente porque em alguma etapa desse tratamento intervenções humanas podem estar presentes.

Por isso, é mal negócio para empresas desse setor não se valerem de ajuda especializada pra se adequarem às novas condutas que deverão tomar a partir de 2021.

Nesse trabalho, a partir do terceiro capítulo, propomos a estruturação de um programa de compliance voltado para o tratamento de dados pessoais sensíveis como forma de ajudar essas empresas do setor da saúde.

Foi observado que passada a fase inicial de estruturação do risco de compliance, a atenção do programador deveria ser direcionada ao código de conduta e ao código de ética, haja vista que o maior desafio nesse programa em específico é a lida entre pacientes e os profissionais envolvidos, uma vez que

ainda não é comum tecnologias onde o paciente é atendido por robôs ou máquinas interativas, e ainda que fosse, seria inviável a falta de interação humana nos casos de emergência médica, por exemplo.

Além do foco no código de conduta e no código de ética, o operador do programa terá que focar com prioridade na execução desses dois pilares, tendo em vista o paciente passar por vários setores com várias pessoas até receber sua alta: secretaria, triagem, consulta médica, setor de exames, internação, acompanhamento e alta, por exemplo. Se cada funcionário do seu respectivo setor não estiver devidamente treinado na coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração, conforme a necessidade estudada previamente para o setor, então haverá sérios risco do programa estar comprometido e as informações vazarem sem se saber exatamente de onde partiu a falha.

Um terceiro foco que o programador deve ter está na reprodução de modelos que funcionam ao redor do mundo, como é o caso dos princípios de Caldicott, voltados exclusivamente para proteção dos dados dos pacientes no Reino Unido. Claro que adaptações precisam ser feitas para adequar o programa a realidade brasileira, mas é inegável a maturidade dos referidos princípios, uma vez que vem sendo aplicados como um verdadeiro “compliance” desde 1997 com reconhecido sucesso, elevando tais diretrizes a um padrão de excelência global.

Por fim, e talvez o mais importante, o programador deverá ter zelo na aquisição do consentimento do uso dos dados sensíveis por parte do usuário/paciente. Sem esse consentimento, pode-se dizer que o tratamento de dados pessoais ficará adstrito a poucos dados, que independem de consentimento, mas que também não revelarão muita coisa da vida do paciente, caso a intenção da empresa seja o melhoramento de serviços e produtos.

Embora seja indispensável para fins econômicos, nem sempre esse consentimento será de fácil aquisição. Primeiro porque é fato notório que os hospitais lidam com emergências constantemente, não sendo possível fazer qualquer abordagem com o paciente em estado crítico e também não sendo possível aferir com precisão se a pessoa que lhe acompanha está dotada de poderes suficientes para autorizar o tratamento de dados do acompanhado.

Segundo por o usuário/paciente ter ganhado da nova legislação a faculdade de fornecer os dados que achar conveniente, não sendo mais possível o tratamento de dados que não estejam devidamente consentidos.

No primeiro caso, uma estratégia interessante seria treinar todos os profissionais dos setores que o paciente passará para perceberem a oportunidade de requerer o consentimento para uso dos dados, quando a emergência tiver passado, obviamente, ou, nos casos de grandes demandas, ter um funcionário que acompanhará todos os setores e na oportunidade que se abrir para abordar mais tranquilamente o paciente, fazer o requerimento do consentimento para uso dos dados.

No segundo caso, a estratégia seria trabalhar no marketing, na venda da ideia. Nesses casos em específico, onde de um lado se tem um paciente que não é obrigado a fornecer nenhum dado se não quiser, e, do outro, empresas que dependem desses dados para aperfeiçoarem seus produtos e/ou serviços, a melhor saída será, sem dúvida, a venda dos benefícios do consentimento.

Como aludido no item 4.3, a dinâmica dessas empresas não permitem o luxo de se ter um funcionário que se sente junto ao paciente para explicar-lhe sobre a nova lei geral, os benefícios em consentir com o uso dos dados, os cuidados que a empresa tem com a privacidade e etc.. Por isso, acreditamos que uma saída prática e barata, que deverá estar integrada ao programa de compliance, seria na abordagem por formulário junto ao paciente ou seu representante legal.

O desafio desse formulário seria unir a venda, o marketing, os benefícios e a segurança com a privacidade tudo num único lugar, tudo isso com linguagem simples e direta, com opções de escolhas que vão para além de “sim” ou “não” (sempre que possível).

Com um formulário nesses termos, haverá uma tendência na facilitação do consentimento por parte do consumidor/paciente, tendo em vista que se estará lhe dando a sensação almejada pela legislação de proteção de dados: a de que está no controle dos seus dados e os dispõe da forma que quiser e para quem quiser, atenuando o medo em consentir acesso a terceiros de dados tão íntimos.

Pelo exposto, a presente pesquisa concluiu seu dever em apontar uma solução para um problema real que infligirá muitas empresas do setor da saúde. Ao mesmo tempo, mostrou que uma grande oportunidade de mercado surgirá,

principalmente para quem lida com o compliance ou atua junto a empresas com esse perfil, se tornando, por fim, numa boa fonte de consulta para estudos posteriores e/ou para orientações práticas na estruturação de um eficiente programa de integridade voltado para a demanda do setor da saúde.

REFERÊNCIAS

ACESS TO EUROPEAN UNION LAW. Directiva 95/46/CE do Parlamento Europeu e do Conselho, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. **EUR-Lex**, 24 out. 1995. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046>. Acesso em: 18 set. 2020.

_____. Diretiva (EU) 2016/680 do Parlamento Europeu e do Conselho relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. **EUR-Lex**, 27 abr. 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L0680.>. Acesso em: 18 set. 2020.

_____. Regulamento (CE) 45/2001 do Parlamento Europeu e do Conselho, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados.18 dez. 2000. **EUR-Lex,** 10 dez. 2018. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32001R0045>. Acesso em: 18 set. 2020.

_____. Directiva 2000/31/CE do Parlamento Europeu e do Conselho, relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio electrónico, no mercado interno. 08 jun. 2000. **EUR-Lex,** 08 jun. 2000. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32000L0031>. Acesso em: 18 set. 2020.

ALJAREH, Salem; DOBSON, John; ROSSITER, Nick. **Satisfaction of Health Record Security Principles through Collaborative Protocols**. Disponível em: <http://nickrossiter.org.uk/process/brazil2003.pdf>. Acesso em: 03 jun. 2020.

ARAUJO, Luiz Alberto David; NUNES JÚNIOR, Vidal Serrano. **Curso de Direito Constitucional**. 9. ed. São Paulo: Saraiva, 2005.

ARAÚJO, Tarso. Verdades inconvenientes sobra a indústria dos remédios. **Super Interessante**, 16 mai. 2018. Disponível em: <https://super.abril.com.br/saude/verdades-inconvenientes-sobre-a-industria-dos-remedios/>. Acesso em: 18 set. 2020.

ASIA-PACIFIC ECONOMIC COOPERATION – APEC. Privacy Framework. **APEC**. Disponível em: <https://www.apec.org/search?Query=Privacy+Framework>. Acesso em: 18 set. 2020.

BANDAROVSKY, Bruno Pires. **Compliance Risk Assessment em 8 passos**. Disponível em: <http://conteudo.lec.com.br/compliance-risk-assessment-em-8-passos>. Acesso em: 02 jun. 2020.

BBC. Caso do Facebook e Cambridge Analytica. **G1**, 20 mar. 2018. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml> Acesso em: 18 set. 2020.

BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. **Proteção de dados e privacidade:** do direito às novas tecnologias na sociedade da informação. Rio de Janeiro: Lumen Juris, 2018

BRASIL. Brasília. **Constituição da República Federativa do Brasil de 1988.** Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 18 set. 2020.

_____. **Decreto nº 3.678, de 30 de novembro de 2000**. Promulga a Convenção sobre o Combate da Corrupção de Funcionários Públicos Estrangeiros em Transações Comerciais Internacionais, concluída em Paris, em 17 de dezembro de 1997. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D3678.htm>. Acesso em: 27 mai. 2020.

_____. **Decreto nº 4.829, de 3 de setembro de 2003**. Dispõe sobre a criação do Comitê Gestor da Internet no Brasil - CGI.br, sobre o modelo de governança da Internet no Brasil, e dá outras providências. Disponível em: <https://cgi.br/pagina/decretos/108>. Acesso em: 18 set. 2020.

_____. **Decreto nº 7.962, de 15 de março de 2013**. Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D7962.htm>. Acesso em: 18 set. 2020.

_____. **Decreto nº 18.956, de 22 de outubro de 1929**. Promulga seis convenções de direito internacional publico, approvadas pela Sexta Conferencia internacional americana. Disponível em: <https://www2.camara.leg.br/legin/fed/decret/1920-1929/decreto-18956-22-outubro-1929-549004-publicacaooriginal-64267-pe.html>. Acesso em: 30 abri. 2020.

_____. **Decreto-Lei nº 4.657, de 04 de setembro de 1942**. Lei de Introdução às normas do Direito Brasileiro. Disponível em: <www.planalto.gov.br/ccivil_03/decreto-lei/Del4657compilado.htm>. 18 set. 2020.

_____. **Lei nº 8.078/90, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em: 18 set. 2020.

_____. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm>. Acesso em: 18 set. 2020.

_____. **Lei nº 12.414, de 09 de junho de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: <www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm>. Acesso em: 18 set. 2020.

_____. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 18 set. 2020.

_____. **Lei nº 12.737, de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 18 set. 2020.

_____. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em:<http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 18 set. 2020.

_____. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm> Acesso em: 18 set. 2020.

_____. **Lei nº 13.853, de 8 de julho de 2019.** Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm> Acesso em: 18 set. 2020.

_____. **Medida Provisória 869, 22 de dezembro de 2018**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2190283>. Acesso em: 06 fev. 2020.

BRASIL. **Medida Provisória 959, de 29 de abril de 2020**. Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória nº 936, de 1º de abril de 2020, e prorroga a vacatio legis da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais. Disponível em: <http://www.in.gov.br/web/dou/-/medida-provisoria-n-959-de-29-de-abril-de-2020-254499639>. Acesso em: 26 jun. 2020.

_____. **Projeto de Lei nº 5.276, apresentado em 13 de maio de 2016**. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>. Acesso em: 18 set. 2020.

_____. **Projeto de Lei nº 5.762, apresentado em 30 de outubro de 2019**. Altera a Lei nº 13.709, de 2018, prorrogando a data da entrada em vigor de dispositivos da Lei Geral de Proteção de Dados Pessoais - LGPD - para 15 de agosto de 2022. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2227704>. Acesso em: 18 set. 2020.

_____. **Proposta de emenda à Constituição nº 17, de 2019**. Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1564052658918&disposition=inline>. Acesso em: 18 set. 2020.

_____. Ministério do Planejamento, Orçamento e Gestão. **Estratégia de Governança Digital da Administração Pública Federal.** Brasília: MP, 2016.

BONAVIDES, Paulo. **Curso de Direito Constitucional**. 15 ed. Malheiros: São Paulo, 2004.

BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. **Proteção de dados e privacidade:** do direito às novas tecnologias na sociedade da informação. Rio de Janeiro: Lumen Juris, 2018.

BRITTO, Érica Apgaua. Governança e accountability no setor público: auditoria operacional como instrumento de controle das ações públicas a cargo do TCEMG. **Revista TCEMG**. 2014. Disponível em: <https://revista1.tce.mg.gov.br/Content/Upload/Materia/2421.pdf>. Acesso em: 01 jun. 2020.

CAMBRIDGE DICTIONARY. **To comply**. Disponível em: <https://dictionary.cambridge.org/pt/dicionario/ingles/comply>. Acesso em: 27 mai. 2020.

CAPELAS, Bruno. Facebook perde US$ 128 bi em valor de mercado e vê conta de escândalos chegar. **Estadão**, 25 jul. 2018. Disponível em: <https://link.estadao.com.br/noticias/empresas,acoes-do-facebook-caem-20-apos-queda-em-crescimento-de-usuarios,70002415365>. Acesso em: 18 set. 2020.

CARVALHO, Julia. Quem é a empresa que lucra juntando dados sobre sua saúde. **Exame**, 06 jan. 2014. Disponível em: <https://exame.abril.com.br/negocios/quem-e-a-empresa-que-lucra-juntando-dados-sobre-sua-saude/>. Acesso em: 18 set. 2020.

CARVALHO, Vinicius Marques; MENDES, Francisco Schertel. **Compliance**: concorrência e combate à corrupção. São Paulo: Trevisan Editora, 2017, *E-book*.

CASTRO, Luiz Fernando Martins. **Proteção de dados pessoais** – internacional e brasileiro. Disponível em: <https://revistacej.cjf.jus.br/revcej/article/view/506/687>. Acesso em: 03 mai. 2020.

CNPD – Comissão Nacional de Proteção de Dados. **Carta dos Direitos Fundamentais da União Europeia**. Disponível em: <https://www.cnpd.pt/bin/legis/internacional/CARTAFUNDAMENTAL.pdf>. Acesso em: 18 set. 2020.

COIMBRA, Marcelo de Aguiar (Org.); MANZI, Vanessa Alessi (Org.). **Manual de Compliance**: preservando a boa governança e a integridade das organizações. São Paulo: Editora Atlas S.A, 2010.

COMISSAO DAS COMUNIDADES EUROPEIAS. **Comunicação da Comissão relativa ao princípio da precaução.** Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:52000DC0001>. Acesso em 06 fev. 2020.

COMPUTERS using digital footprints are better judges of personality than firends and family. **University of Cambridge**. Disponível em: https://www.cam.ac.uk/research/news/computers-using-digital-footprints-are-better-judges-of-personality-than-friends-and-family. Acesso em: 18 set. 2020.

CONSELHO FEDERAL DE MEDICINA - CFM. **Resolução CFM nº 2.227/2018, de 13 de dezembro de 2018**. Define e disciplina a telemedicina como forma de prestação de serviços médicos mediados por tecnologias. Disponível em: <http://portal.cfm.org.br/images/PDF/resolucao222718.pdf>. Acesso em: 02 jun. 2020.

CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. **Compliance:** Perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018.

CUNHA, Matheus; KALAY, Marcio El. **Manual de Compliance**: Compliance Mastermind Vol. 1. São Paulo: Lec Editora, 2019.

CUSTÓDIO, Mônica. Conheça as 10 redes sociais mais usadas no Brasil. **Resultados Digitais**, 11 fev. 2019. Disponível em: <https://resultadosdigitais.com.br/blog/redes-sociais-mais-usadas-no-brasil/>. Acesso em: 18 set. 2020.

DEPARTMENT OF JUSTICE EUA. **Evaluation of Corporate Compliance Programs**. Disponível em: <https://www.justice.gov/criminal-fraud/page/file/937501/download>. Acesso em: 29 mai. 2020.

DEPARTMENT OF JUSTICE EUA; SECURITIES AND EXCHANGE COMMISSION. **FCPA**: A Resource Guide to the U.S. Foreing Corrupt Practices Act. Disponível em: <https://www.sec.gov/spotlight/fcpa/fcpa-resource-guide.pdf>. Acesso em: 03 jun. 2020.

_____. **Foreing Corrupt Practices Act**. Disponível em: <https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act>. Acesso em: 27 mai. 2020.

DETRAN deixa vazar dados de 60 milhões de brasileiros com CNH. **Estadão**, 14 out. 2019. Disponível em: <https://jornaldocarro.estadao.com.br/carros/detran-vaza-dados-70-milhoes-brasileiros/>. Acesso em: 18 set. 2020.

DONEDA, Danilo. **A Lei Geral de Proteção de Dados Pessoais**. In: Congresso Internacional da Propriedade Intelectual da Associação Brasileira da Propriedade Intelectual - ABPI, XXXVIII, 2018, São Paulo. Disponível em: <http://www.abpi.org.br/congressosdaabpi/pos-evento/2018/apresentacoes/painel7/Danilo%20Doneda.pdf>. Acesso em: 18 set. 2020.

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

DONEDA, Danilo. **O direito fundamental à proteção de dados pessoais**. MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Orgs). Direito Digital: direito privado e internet. 2. ed. São Paulo: Foco, 2019.

DONEDA, Danilo; MENDES, Laura Shertel. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**. Ano 27. vol. 120. São Paulo: Revista dos Tribunais, 2018.

DUCAN, Sawyer. **William Dudley Addresses the Importance of Corporate Culture**. Disponível em: <https://www.kslaw.com/blog-posts/new-york-feds-william-dudley-addresses-the-importance-of-corporate-culture>. Acesso em: 29 mai. 2020.

DUHIGG, Charles. **O Poder do Hábito**: por que fazemos o que fazemos na vida e nos negócios. Tradução Rafael Mantovani. Rio de Janeiro: Objetiva, 2017.

ENDEAVOR. **Prevenindo com o Compliance para não remediar com o caixa**. Disponível em: <https://endeavor.org.br/pessoas/compliance/>. Acesso em: 29 mai. 2020.

EUROPEAN COMMISSION. **Answer**. Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en>. Acesso em: 18 set. 2020.

_____. **Data protection**: rules for the protection of personal data inside and outside the EU. Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection_en>. Acesso em: 18 set. 2020.

EUROPEAN COURT OF HUMAN RIGHTS - ECHR. **Convenção Europeia dos Direitos do Homem**. Disponível em: <https://www.echr.coe.int/Documents/Convention_POR.pdf>. Acesso em: 15 abr. 2020.

EUROPEAN DATA PROTECTION BOARD. **Guidelines 05/2020 on consent under Regulation 2016/679**. Disponível em: <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf>. Acesso em: 25 jun. 2020

EXCLUSIVO: Investigação da BandNews FM revela venda de dados pessoais. **BandNews FM**, 23 abr. 2019. Disponível em: <http://www.bandnewsfm.com.br/2019/04/23/exclusivo-investigacao-da-bandnews-fm-revela-venda-de-dados-pessoais/>. Acesso em: 18 set. 2020.

FACEBOOK eleva para 87 milhões o nº de usuários que tiveram dados explorados pela Cambridge Analytica. **G1**, 04 abri. 2018. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/facebook-eleva-para-87-milhoes-o-n-de-usuarios-que-tiveram-dados-explorados-pela-cambridge-analytica.ghtml>. Acesso em: 18 set. 2020.

FERNANDES, Matheus Hetterich; TAMBOSI, Juliete. Qual o valor dos seus dados pessoais na internet? **Wlive**. Disponível em: <https://wlive.com.br/post/qual-o-valor-dos-seus-dados-pessoais-na-internet-734>. Acesso em: 18 set. 2020.

FERREYRA, Eduardo. **Legislación argentina sobre protección de datos personales**. Disponível em: <https://adcdigital.org.ar/wp-content/uploads/2017/01/Legislacion-argentina-sobre-proteccion-de-datos-personales-ADC.pdf>. Acesso em: 18 set. 2020.

FERREIRA, Keila Pacheco; RODRIGUES, Yuri Gonçalves dos Santos. **A privacidade no ambiente virtual**: avanços e insuficiências da Lei Geral de Proteção de Dados no Brasil (Lei 13.709/18). Revista de Direito do Consumidor. vol. 122. ano 28. São Paulo: RT, 2019.

FONSECA, João José Saraiva. **Metodologia da pesquisa científica**. Disponível em: <http://www.ia.ufrrj.br/ppgea/conteudo/conteudo-2012-1/1SF/Sandra/apostilaMetodologia.pdf> Acesso em: 18 set. 2020.

FOUQUET, Helene; GRANT, Nico; LI, Dandan; MAWAD, Marie. Venda de dados pessoais é o próximo passo da revolução de big data. **Bloomberg**, 8 de jun. de 2018. Disponível em: <https://www.bloomberg.com.br/blog/venda-de-dados-pessoais-e-proximo-passo-da-revolucao-de-big-data/>. Acesso em: 18 set. 2020.

FRAZÃO, Ana. Nova LGPD: balanço preliminar da MP 869/2018. **Jota**, 06 de fev. de 2019. Disponível em: <https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-balanco-preliminar-da-mp-869-2018-06022019>. Acesso em: 18 set. 2020.

FROST & SULLIVAN. **The Global State of Online Digital Trust**. Disponível em: <https://www.ca.com/content/dam/ca/us/files/white-paper/the-global-state-of-online-digital-trust.pdf>. Acesso em: 18 set. 2020.

GALINDO, Cristina. Quando as empresas são mais poderosas que os países. **Elpaís**, 08 nov. 2017. Disponível em: <https://brasil.elpais.com/brasil/2017/11/03/economia/1509714366_037336.html> Acesso em: 18 set. 2020.

GERHARDT, Tatiana Engel (Org.); SILVEIRA, Denise Tolfo (Org.). **Métodos de pesquisa**. Rio Grande do Sul: Editora da UFRGS, 2009.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. São Paulo: Atlas, 2007.

GIOVANINI, Wagner. **Compliance**: a excelência na prática. São Paulo: 2014.
GIRÃO, Alexandro. **LGPD e o mito do consentimento para tratamento de dados de saúde**. Disponível em: <https://lec.com.br/blog/lgpd-e-o-mito-do-consentimento-para-tratamento-dos-dados-de-saude/>. Acesso em: 26 jun. 2020.

GODOI, Alexandre Franco de. **Governança Corporativa e Compliance**. Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=&id=blbdDwAAQBAJ&oi=fnd&pg=PT6&dq=governan%C3%A7a+corporativa+e+compliance&ots=Jy8cpjiZUB&sig=B5Mp6BiniFVi7wSWYoQBaZp7no4#v=onepage&q=governan%C3%A7a%20corporativa%20e%20compliance&f=false>. Acesso em: 26 mai. 2020.

GOMES, Helton Simões. Gigantes da tecnologia ganham bilhões com uso de dados de pessoas para distribuir anúncios segmentados. **G1**, 13 abr. 2018. Disponível em:<https://g1.globo.com/economia/tecnologia/noticia/gigantes-da-tecnologia-ganham-bilhoes-com-uso-de-dados-de-pessoas-para-distribuir-anuncios-segmentados.ghtml> Acesso em: 18 set. 2020.

GOMES, Helton Simões. Câmara aprova recriação do “xerife de dados”, órgão protetor da privacidade. **Uol**, 28 mai. 2019. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2019/05/28/camara-aprova-recriacao-do-xerife-de-dados-orgao-protetor-da-privacidade.htm>. Acesso em: 27 mar. 2020.

GOVERNO FEDERAL. **Revisão da Estratégia de Governança Digital**. Disponível em: <http://www.planejamento.gov.br/EGD/arquivos/revisao-da-estrategia-de-governanca-digital-2015-2019.pdf>. Acesso em: 18 set. 2020.

GRAHAM, Helen; GREENOUGH, Anne. **Protecting and using patient information**: the role of the Caldicott Guardian. Disponível em: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4953587/pdf/246.pdf>. Acesso em: 02 jun. 2020.

HARARI, Noah Yuval. **Homo Deus**: uma breve história do amanhã. Rio de Janeiro: Companhia Das Letras, 2015.

HARARI, Noah Yuval. **21 lições para o século 21**. Rio de Janeiro: Companhia Das Letras, 2018.

HERN, Alex. Vibrator maker ordered to pay out c$4m for tracking users’ sexual activity. **The Guardian**, 14 mar. 2017. Disponível em:<https://www.theguardian.com/technology/2017/mar/14/we-vibe-vibrator-tracking-users-sexual-habits>. Acesso em: 18 set. 2020.

HOSPFAR. **Código de Conduta 2018**. Disponível em: <https://www.hospfar.com.br/backend/midias/multipleupload/gc-institucional/09052018170335.pdf>. Acesso em: 31 mai. 2020.

HOSPFAR. **Nossa empresa**: Excelência em distribuição de produtos hospitalares no Brasil. Disponível em: <https://www.hospfar.com.br/nossa-empresa>. Acesso em: 31 mai. 2020.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA - IBGE. **Demografia das empresas**. Disponível em: <https://www.ibge.gov.br/estatisticas/economicas/industria/9068-demografia-das-empresas.html?t=sobre>. Acesso em: 29 mai. 2020.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA - IBGC. **Compliance**: construindo um sistema de conformidade alinhado às melhores práticas de governança corporativa. Disponível em: <http://midias.cnseg.org.br/data/files/C4/03/DB/22/46E006100852FFF5F98AA8A8/IBGC_Compliance_Versao_AP_20171107-PDF.pdf>. Acesso em: 27 mai. 2020.

INSTITUTO ETHOS. **Formulação e Implantação de Código de Ética em empresas:** Reflexões e Sugestões. Disponível em: <https://www.ethos.org.br/wp-content/uploads/2013/05/Elaboracao-Codigo-de-Etica-Ethos-Claudio-Abramo.pdf>. Acesso em: 03 jun. 2020.

INSTITUTE FOR BUSINESS VALUE – IBM. The end of the beginning: unleashing the transformational Power of GDPR. **IBM**, mai. 2018. Disponível em: <https://www.ibm.com/downloads/cas/JEMXN6LV>. Acesso em: 18 set. 2020.

INTERNATIONAL LABOUR OFFICE - ILO. **Protection of worker's personal data**. Disponível em: <https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf>. Acesso em: 01 jun. 2020.

_____. **O que é governança corporativa.** Disponível em: <https://www.ibgc.org.br/conhecimento/governanca-corporativa>. Acesso em: 26 mai. 2020.

_____. **O IBGC.** Disponível em: <https://www.ibgc.org.br/quemsomos>. Acesso em: 26 mai. 2020.

IPDFARMA - Instituto de Pesquisa e Desenvolvimento de Fármacos e Produtos Farmacêuticos. Febrafar anuncia expectativas para o mercado farmacêutico em 2019. **IPDfarma**, 08 jan. 2019. Disponível em: <http://ipd-farma.org.br/noticias/pagina/1229/Febrafar-anuncia-expectativas-para-o-mercado-farmaceutico-em-2019>. Acesso em: 18 set. 2020.

KPMG. **Pesquisa**: Maturidade do *Compliance* no Brasil: Desafio das empresas no processo de estruturação da função e programa de *compliance* na prevenção, na detecção e no monitoramento dos riscos. 2015, *E-book*.

KEEN, Andrew. **Vertigem digital:** por que as redes sociais estão nos dividindo, diminuindo e desorientando. Rio de Janeiro: Zahar, 2012.

KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon; NEGRI, Sergio Marcos Carvalho de Ávila. **A normatividade dos dados sensíveis na Lei Geral de Proteção de Dados**: ampliação conceitual e proteção da pessoa humana. Disponível em: <https://indexlaw.org/index.php/revistadgnt/article/view/5479/pdf>. Acesso em: 03 mai. 2020.

KOSINSK, Michal; STILLWELL, David; GRAEPEL, Thore. Private trais and attributes are predictable from digital records of human behavior. **PNAS,** 09 abr. 2013. Disponível em: <https://www.pnas.org/content/110/15/5802>. Acesso em: 18 set. 2020.

LANEY, Doug. **3D Data Management**: Controlling Data Volume, Velocity, and Variety. Disponível em: <https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf>. Acesso em: 18 set. 2020.

LEINER, Barry M. et. al. **Brief History of the Internet**. Disponível em: <https://www.internetsociety.org/internet/history-internet/brief-history-internet/>. Acesso em: 15 de abr. 2020.

LIEDKE, Mônica Souza; SCHIOCCHET, Taysa. O direito e a proteção das gerações futuras na sociedade de risco global. **Revista Veredas do Direito**. V. 9. n. 17. Janeiro/Junho. Belo Horizonte, 2012.

LUCA, Cristina De. Senado aprova proteção de dados pessoais como direito fundamental. **Porta23**, 03 jul. 2019. Disponível em: https://porta23.blogosfera.uol.com.br/2019/07/03/senado-aprova-protecao-de-dados-pessoais-como-direito-fundamental/. Acesso em: 18 set. 2020.

LUIZ, Gabriel. CPF em troca de desconto: MP investiga venda de dados de clientes por farmácias. **G1**, 16 mar. 2018. Disponível em: <https://g1.globo.com/df/distrito-federal/noticia/cpf-em-troca-de-desconto-mp-investiga-venda-de-dados-de-clientes-por-farmacias.ghtml>. Acesso em: 18 set. 2020.

MALDONADO, Viviane Nóbrega et al. **LGPD**: Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters, 2019.

MARINONI, Luiz Guilherme; MITIDIERO, Daniel; SARLET, Ingo Wolfgang. **Curso de Direito Constitucional**. 6.ed. Saraiva: São Paulo, 2017.

MARTINS, Guilherme Magalhães (Coord.); LONGHI, João Victor Rozatti (Coord.). **Direito digital**: direito privado e internet. 2. ed. São Paulo: Editora Foco, 2019.

MATOS, Tiago Farina. **Comércio de dados pessoais, privacidade e Internet**. Disponível em: <file:///C:/Users/Tiago%20Soares/Desktop/Artigo%20par%20ao%20mestrado%20-%20.pdf>. Acesso em: 18 set. 2020.

MAUES, Antonio Morreira. **Supralegalidade dos tratados internacionais de direitos humanos e interpretação constitucional**. Disponível em: <http://www.corteidh.or.cr/tablas/r32493.pdf>. Acesso em: 23 mai. 2020.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MIGUEL, Inês Pinto. Cambridge Analytica não foi paga mas envolveu-se na campanha do “Leave”. **Jornal Económico**, 20 jul. 2019. Disponível em: <https://jornaleconomico.sapo.pt/noticias/cambridge-analytica-nao-foi-paga-mas-envolveu-se-na-campanha-do-leave-473567>. Acesso em: 18 set. 2020.

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES. **E-Digital**: estratégia brasileira para a transformação digital. Disponível em: <http://www.mctic.gov.br/mctic/export/sites/institucional/arquivos/ASCOM_PUBLICACOES/estrategia_digital.pdf>. Acesso em: 18 set. 2020.

MINISTRY OF JUSTICE. **Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing**. Disponível em: <http://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf>. Acesso em: 03 jun. 2020.

MORAES, Maria Celina Bodin de. **A vida na sociedade de vigilância:** privacidade hoje. Rio de Janeiro: Renovar, 2008.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). **Revista de Direito e Garantias Fundamentais**. v. 19. n. 3. Disponível em: <http://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603/pdf>. Acesso em: 18 set. 2020.

MURINO, Thiago Barrizzelli. **O consentimento válido nas novas leis de proteção de dados**. Disponível em: <https://www.migalhas.com.br/depeso/286214/o-consentimento-valido-nas-novas-leis-de-protecao-de-dados>. Acesso em 25 jun. 2020.

NAÇÕES UNIDAS. **Convenção das Nações Unidas contra a corrupção**. Disponível em: <https://www.unodc.org/documents/lpo-brazil/Topics_corruption/Publicacoes/2007_UNCAC_Port.pdf>. Acesso em: 27 mai. 2020.

NATIONAL HEALTH SERVICE - NHS. **Confidentiality**: NHS Code of Practice. Disponível em: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf>. Acesso em: 03 jun. 2020.

NEVES, Leonardo Meyohas. **Cláusulas Pétreas na Constituição da República Federativa do Brasil de 1988**. Disponível em: <http://www.emerj.tjrj.jus.br/paginas/trabalhos_conclusao/2semestre2014/trabalhos_22014/LeonardoMeyohasNeves.pdf>. Acesso em: 18 set. 2020.

NHS. What are the Caldicott Principles? Disponível: <https://www.igt.hscic.gov.uk/Caldicott2Principles.aspx>. **NHS**. Acesso em: 18 set. 2020.

NOVARTIS. **Código de Conduta**. Disponível em: <https://www.novartis.com.br/sites/www.novartis.com.br/files/documents/C%C3%B3digo%20de%20Conduta%20da%20Novartis%20%28v3-2019%29.pdf>. Acesso em: 03 jun. 2020.

OGLOBO. Intel: 80% das pessoas dormem com celular e 40% atendem às ligações no até no banheiro. **OGlobo**, 05 abri. 2012. Disponível em:

<https://oglobo.globo.com/economia/intel-80-das-pessoas-dormem-com-celular-40-atendem-as-ligacoes-ate-no-banheiro-4506027>. Acesso em: 18 set. 2020.

OLIVIERI, Nicolau. LGPD: impactos nas rotinas trabalhistas e no contrato de trabalho: O trabalho das empresas está só começando. **Jota**, São Paulo, 14 maio 2019. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/lgpd-impactos-nas-rotinas-trabalhistas-e-no-contrato-de-trabalho-14052019>. Acesso em: 18 set. 2020.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos** – DHUDH. 1948. Disponível em:< https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf> Acesso em: 18 set. 2020.

ORGANIZATION OF AMERICAN STATES - OAS. **Convención de Viena sobre el derecho de los tratados**. Disponível em: <https://www.oas.org/xxxivga/spanish/reference_docs/Convencion_Viena.pdf>. Acesso em: 30 abr. 2020.

_____. **Convenção Interamericana contra a Corrupção**. Disponível em: <http://www.oas.org/juridico/portuguese/treaties/B-58.htm>. Acesso em: 27 mai. 2020.

_____. **Convenio 108 del Consejo de Europa**. Disponível em: <https://www.oas.org/es/sla/ddi/docs/U12%20convenio%20n%20108.pdf>. Acesso em: 15 abri. 2020.

_____. **Pacto Internacional dos Direitos Civis e Políticos (1966)**. Disponível em: <https://www.oas.org/dil/port/1966%20Pacto%20Internacional%20sobre%20Direitos%20Civis%20e%20Pol%C3%ADticos.pdf>. Acesso em: 15 abr. 2020.

ORGANIZAÇÃO MUNDIAL DA SAÚDE - OMS. **Medição da saúde digital. Recomendações metodológicas e estudo de caso.** Disponível em: <https://www.cetic.br/media/docs/publicacoes/11/medicao%20da%20saude%20digital.pdf>. Acesso em 01 mai. 2020. Comitê Gestor da Internet no Brasil – CGI.br SÃO PAULO, 2018

ORWELL, George. **1984**. Tradução Alexandre Hubner e Heloisa Jahn. São Paulo: Companhia das Letras, 2017.

PAIVA, Maristela. **Impactos da gestão estratégica no trabalho da Secretaria de Controle Interno da Câmara dos Deputados**. Disponível em: <http://bd.camara.gov.br/bd/handle/bdcamara/3785>. Acesso em: 01 jun. 2020.

PARLAMENTO EUROPEU; CONSELHO DA UNIÃO EUROPEIA. **Regulamento (UE) 2016/679, de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>. 26 jun. 2020.

_____. **Directiva 2006/24/CE, de 15 de março de 2006**. Relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva 2002/58/CE. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:32006L0024>. Acesso em: 15 abr. 2020.

_____. **Diretiva 95/46/CE, de 24 de outubro de 1995**. Relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046>. Acesso em: 15 abr. 2020.

_____. **Diretiva 97/66/CE, de 15 de dezembro de 1997**. Relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das telecomunicações. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A31997L0066>. Acesso em: 16 abr. 2020.

PARLIAMENTARY ASSEMBLY. **Declaration on mass communication media and Human Rights. Resolution 428 (1970)**. Disponível em: <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=15842&lang=en.>. Acesso em: 15 abr. 2020.

PESQUISA sobre Confiança Digital indica que 43% dos executivos de negócios admitem vender dados de seus consumidores. **CRYPTOID**, 11 set. 2018. Disponível em: <https://cryptoid.com.br/ciberseguranca-seguranca-da-informacao/pesquisa-sobre-confianca-digital-indica-que-43-dos-executivos-de-negocios-admitem-vender-dados-de-seus-consumidores/>. Acesso em: 18 set. 2020.

PINHEIRO, Bárbara Santini. **O que estão fazendo com os meus dados? A importância da Lei Geral de Proteção de Dados**. Cood. Paloma Mendes Saldanha. E-book. OAB Pernambuco. Recife: SerifaFina, 2019.

PINHEIRO, Patricia Peck. Nova Lei Brasileira de Proteção de Dados Pessoais (LGPD) e o impacto nas instituições públicas e privadas. **RT 1.000**. Ano 108. vol. 1.000. São Paulo: Revista dos Tribunais, 2019.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais**: comentários a lei n. 13.709/2018. São Paulo: Saraiva, 2018.

PINHEIRO, Valter Luis Macedo de Carvalhaes. O crescimento da indústria farmacêutica. **Panorama Farmacêutico**, 11 out. 2019. Disponível em: <https://panoramafarmaceutico.com.br/2019/10/11/o-pujante-crescimento-da-industria-farmaceutica/>. Acesso em: 18 set. 2020.

PIOVESAN, Flávia. **Tratados internacionais de proteção dos direitos humanos**: jurisprudência do STF. Disponível em: <http://www.oas.org/es/sadye/inclusion-social/protocolo-ssv/docs/piovesan-tratados.pdf>. Acesso em 23 mai. 2020.

PONEMON INSTITUTE. **The true cost of compliance**: a Benchmark Study of Multinational Organizations. Ponemon Institute: 2011, *E-book*.

RED cross blood service admits to personal data breach affecting half a million donors. **ABCNEWS**, 28 out. 2016. Disponível em: <https://www.abc.net.au/news/2016-10-28/red-cross-blood-service-admits-to-data-breach/7974036>. Acesso em: 18 set. 2020.

REUTERS. Facebook pagará multa recorde de US$ 5 bi para encerrar investigações sobre vazamento dados para Cambridge Analytica. **OGlobo**, 24 jul. 2019. Disponível em: <https://oglobo.globo.com/economia/tecnologia/facebook-pagara-multa-recorde-de-us-5-bi-para-encerrar-investigacao-sobre-vazamento-de-dados-para-cambridge-analytica-23828387>. Acesso em: 18 set. 2020.

RODOTÀ, Stefano. **A vida na sociedade de vigilância**: privacidade hoje, Rio de Janeiro: Renovar, 2008.

RODRIGUEZ, Daniel Piñeiro; RUARO, Regina Linden. O direito à proteção de dados pessoais: uma leitura do sistema europeu e a necessária tutela dos dados sensíveis como paradigma para um sistema jurídico brasileiro. **Revista Brasileira de Direitos Fundamentais e Justiça**. Ano 4. n. 11. Porto Alegre: HS Editora, 2010.

SANTOS, Fabíola Meira de Almeida; TALIBA, Rita. **Lei Geral de Proteção de Dados no Brasil e os possíveis impactos.** Revista dos Tribunais. vol. 988. Ano 107. São Paulo: RT, 2018.

SANTOS, Juliana Graciela dos. **Antecedentes dos benefícios percebidos de compliance às políticas de proteção de dados pessoais nas organizações.** Disponível em: <http://tede.metodista.br/jspui/bitstream/tede/1612/2/JulianaG.Santos.pdf>. Acesso em: 01 jun. 2020.

SARMENTO, Daniel. **Dignidade da pessoa humana**: conteúdos, trajetórias e metodologia. Editora Forúm: Belo Horizonte, 2016.

SERVIÇO BRASILEIRO DE APOIO ÀS MICRO E PEQUENAS EMPRESAS - SEBRAI. ***Causa Mortis***: o sucesso e o fracasso das empresas nos primeiros 5 anos. Disponível em: <https://m.sebrae.com.br/Sebrae/Portal%20Sebrae/UFs/SP/Anexos/causa_mortis_2014.pdf>. Acesso em: 29 mai. 2020.

SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS – SERPRO. Quem vai regular a LGPD? **Serpro**. Disponível em: <https://www.serpro.gov.br/lgpd/governo/quem-vai-regular-e-fiscalizar-lgpd>. Acesso em: 27 mar. 2020.

SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS – SERPRO. Tirando algumas situações previstas na LGPD, é você, cidadão, que define se seus dados

pessoais podem ou não ser tratados por terceiros. **Serpro**. Disponível em: <https://www.serpro.gov.br/lgpd/cidadao/seu-consentimento-e-lei>. Acesso em: 25 jun. 2020.

SILVA, Alberto [et al.]; organizado por Jhessica Reia [et al.]. **Horizonte presente**: tecnologia e sociedade em debate. Belo Horizonte: Casa doDireito; FGV – Fundação Getúlio Vargas, 2019.

SILVA, Cedê. Nova Lei de Proteção de Dados adianta cargos e adia aplicação. **O Antagonista**, 13 jul. 2019. Disponível em: <https://www.oantagonista.com/comentarista/nova-lei-protecao-de-dados/>. Acesso em: 18 set. 2020.

SILVA, Daniel. Cuidado: seus dados pessoais estão à venda. **Estadão**, 12 fev. 2012. Disponível em: <https://www.estadao.com.br/blogs/jt-seu-bolso/2012/02/12/cuidado-seus-dados-pessoais-estao-a-venda/> Acesso em: 18 set. 2020.

SOARES, Matias Gonsales. **A Quarta Revolução Industrial e seus possíveis efeitos no direito, economia e política**. Disponível em: <https://www.migalhas.com.br/arquivos/2018/4/art20180427-05.pdf>. Acesso em: 18 set. 2020.

SOARES, Pedro Silveira Campos. **A questão do consentimento na Lei Geral de Proteção de Dados**. Disponível em: <https://www.conjur.com.br/2019-mai-11/pedro-soares-questao-consentimento-lei-protecao-dados>. Acesso em: 26 jun. 2020.

TEAM, IT Governance Privacy. **EU General Data Protection Regulation (GDPR):** Na Implementation and Compliance Guide. Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=&id=hnQ2DwAAQBAJ&oi=fnd&pg=PA1&dq=GDPR+commentary&ots=WiNiwyURUt&sig=ObvLKFAvf0O7p7VfAckq1LLM_yY#v=onepage&q=GDPR%20commentary&f=false>. Acesso em: 16 abr. 2020.

TECMUNDO. #BrasilExposed: a crise de segurança na internet brasileira. **TECMUNDO**, 30 mai. 2015. Disponível em: <https://www.tecmundo.com.br/privacidade/80767-brasilexposed-crise-seguranca-internet-brasileira.htm>. Acesso em: 18 set. 2020.

UK CALDICOTT GUARDINA COUNCIL. Manual of Caldicott Guardians. **Gov.UK**. Disponível em: <https://www.gov.uk/government/groups/uk-caldicott-guardian-council#Manual-for-Caldicott-Guardians>. Acesso em: 02 jun. 2020.

UK CORPORATE GOVERNANCE CODE - UKCGC. **The UK Caldicott Guardian Council is the national body for Caldicott Guardians**. Disponível em: <https://www.ukcgc.uk/>. Acesso em: 02 jun. 2020.

VARGAS, Angelo Miguel de Souza. **O bloco de constitucionalidade**: reconhecimento e consequências no Sistema Constitucional Brasileiro. Disponível em: <https://tede.pucsp.br/bitstream/handle/7774/1/angelo.pdf>. Acesso em: 23 mai. 2020.

VELOSO, Thássius. Anatel vai saber tudo sobre os assinantes de telefonia. **Tecnoblog**. Disponível em: <https://tecnoblog.net/54437/anatel-vai-saber-tudo-sobre-os-assinantes-de-telefonia/>. Acesso em: 18 set. 2020.

VILAROUCA, Márcio Grijó; RIBEIRO, Ludmila Mendonça Lopes. **Quando devo fazer pesquisa por meio de entrevistas, e como fazer.** São Paulo: Saraiva, 2012.

ZANELLA, Liane Carly Hermes. **Metodologia da pesquisa**. Florianópolis: SEaD/UFSC, 2006.

APÊNDICE – FORMULÁRIO DE CONSENTIMENTO PARA USO DOS DADOS PESSOAIS SENSÍVEIS DO CLIENTE/PACIENTE, EM CUMPRIMENTO A NOVA LEI GERAL DE PROTEÇÃO DE DADOS (LEI Nº 13.709/2018)

TERMO DE CONSENTIMENTO

. Explicações ao paciente

Agora, no Brasil, está em vigor a nova Lei Geral de Proteção de Dados (LGPD), a qual exige, no seu art. 7, inciso I, e art. 11, também inciso I, que para as empresas fazerem uso (tratamento de dados[30]) dos chamados "dados pessoais" (principalmente os dados sensíveis, ambos elencados abaixo) necessitam, primeiro, pedir o consentimento do paciente/cliente (ou responsável legal), devendo deixar claro, de forma específica e destacada, quais dados estão sendo solicitados e para qual finalidade específica serão usados.

Desse modo, precisamos que você responda as perguntas a seguir para que possamos cumprir as exigências da nova lei:

1.Você consente em recolhermos os seguintes dados pessoais: nome completo; CPF; e-mail (endereço eletrônico); telefone para contato; estado civil; nacionalidade; e naturalidade?

( ) SIM

Com exceção de:_____

( ) NÃO

2.Você consente em usarmos os referidos dados pessoais para as seguintes finalidades: melhoramento dos nossos serviços; ajudar nossos colaboradores no melhoramento de medicamentos; ajudar nossos colaboradores no melhoramento

[30] Art 5º, inciso X, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais): X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

de tratamentos; e criação de um perfil de demanda dos nossos pacientes, de modo a nos orientar onde alocar melhor nossos investimentos?

( ) SIM

Com exceção de:_____

( ) NÃO

3.Você consente em recolhermos os seguintes dados sensíveis: origem racial ou étnica; impedimento de tratamento ou prática médica por causa de convicção religiosa; tipo sanguíneo; doença crônica; doença sexualmente transmissível; uso regular de medicamento(s)?

( ) SIM

Com exceção de:_____

( ) NÃO

4. Você consente em usarmos os referidos dados sensívei para as seguintes finalidades: melhoramento dos nossos serviços; ajudar nossos colaboradores no melhoramento de medicamentos; ajudar nossos colaboradores no melhoramento de tratamentos; e criação de um perfil de demanda dos nossos pacientes, de modo a nos orientar onde alocar melhor nossos investimentos?

( ) SIM

Com exceção de:_____

( ) NÃO

OBS: segundo o inciso II, e alíneas, do art. 11, da LGPD, os referidos dados poderão ser utilizados (tratados) sem necessidade de consentimento do titular ou representante legal quando for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de

pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral; e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Dessa maneira, precisamos que valide esse termo assinando a seguinte afirmativa:

Consinto com o recolhimento e tratamento dos dados pessoais e sensíveis assinalados com “x” entre os itens 1 e 4. _____ Assinatura do titular ou representante legal

_____

Município – Estado, data, mês e ano.

FORMULÁRIO DE COLETA DE DADOS PESSOAIS E SENSÍVEIS

. Dados pessoais

Nome completo do paciente ou responsável legal:
_____

CPF
_____

E-mail (endereço eletrônico)
_____

Telefone para contato
_____

Estado civil
_____

Nacionalidade
_____

Naturalidade
_____

. Dados pessoais sensíveis

Qual sua origem racial ou étnica?
( ) Branca
( ) Negra
( ) Asiática
( ) Outra:
_____

Há algum impedimento de tratamento ou prática médica por causa de convicção religiosa?
( ) Não
( ) Sim, mas não quero falar sobre
( ) Sim e posso dizer qual:
_____

Qual seu tipo sanguíneo?
( ) A +
( ) B +
( ) O +
( ) Não sei
( ) Outro:

_____

Você possui alguma doença crônica?
( ) Não
( ) Sim, mas não quero falar sobre
( ) Sim e posso dizer qual:
_____

Você possui alguma doença sexualmente transmissível?
( ) Não
( ) Sim, mas não quero falar sobre
( ) Sim e posso dizer qual:
_____

Você usa algum medicamento regularmente (a pelo menos 6 meses)?
( ) Não
( ) Sim, mas não quero falar sobre
( ) Sim e posso dizer qual (is):
_____

Agradecemos sua participação.

_____
Município – Estado, data, mês e ano.

_____
Assinatura do paciente ou responsável legal