**PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO**

**Jhesica Loures Dos Santos Baccari**

# O Avanço Tecnológico e a Responsabilidade Social das Empresas na Proteção de Dados Pessoais: Uma abordagem sobre a adoção de medidas de *compliance* com a Lei Geral de Proteção de Dados Pessoais

**MESTRADO EM FILOSOFIA DO DIREITO**

**São Paulo**

**2021**

**Jhesica Loures Dos Santos Baccari**

# O Avanço Tecnológico e a Responsabilidade Social das Empresas na Proteção de Dados Pessoais: Uma abordagem sobre a adoção de medidas de *compliance* com a Lei Geral de Proteção de Dados Pessoais

Dissertação apresentada à Banca Examinadora da Pontifícia Universidade Católica de São Paulo, como exigência parcial para a obtenção do título de MESTRE em Filosofia do Direito, sob a orientação do Prof. Dr. Márcio Pugliesi.

**São Paulo**

**2021**

**Jhesica Loures Dos Santos Baccari**

Autorizo exclusivamente para fins acadêmicos e científicos, a reprodução total ou parcial desta Dissertação de Mestrado por processos de fotocopiadoras ou eletrônicos.

Assinatura Data: 23/06/2021

*e-mail: dra.jhesica@advocaciabaccari.com.br*

Baccari, Jhesica Loures dos Santos

O Avanço Tecnológico e a Responsabilidade Social das Empresas na Proteção de Dados Pessoais: Uma abordagem sobre a adoção de medidas de *compliance* com a Lei Geral de Proteção de Dados Pessoais / Jhesica Loures dos Santos Baccari. – São Paulo (SP), 23.06.2021.
Paginação: 104 fls.

Orientador: Prof. Dr. Márcio Pugliesi.

Dissertação (Mestrado em Filosofia do Direito) -- Pontifícia Universidade Católica de São Paulo, Programa de Estudos Pós-Graduados em Filosofia do Direito, 14.04.2021.
1. Assunto. 2. Assunto. 3. Assunto. I. Sobrenome, Nome do orientador. II. Pontifícia Universidade Católica de São Paulo, Programa de Estudos Pós-Graduados Filosofia do Direito.
O Avanço Tecnológico e a Responsabilidade Social das Empresas na Proteção de Dados Pessoais: Uma abordagem sobre a adoção de medidas de *compliance* com a Lei Geral de Proteção de Dados Pessoais.

**O Avanço Tecnológico e a Responsabilidade Social das Empresas na**

**Proteção de Dados Pessoais:**

**Uma abordagem sobre a adoção de medidas de *compliance* com a Lei Geral**

**de Proteção de Dados Pessoais**

Dissertação apresentada à Banca Examinadora da Pontifícia Universidade Católica de São Paulo, como exigência parcial para a obtenção do título de MESTRE em Filosofia do Direito, sob a orientação do Prof. Dr. Márcio Pugliesi.

Aprovado em: ___/___ /___

BANCA EXAMINADORA

_____

Dr. Márcio Pugliesi

_____

Dra. Clarice Von Oertzen – PUC

_____

Dr. Antônio Márcio da Cunha Guimarães – PUC

_____

Dra. Gabriela Gomes Coelho Ferreira – USP

## AGRADECIMENTOS

O mestrado sempre foi um sonho em minha vida. Era algo muito distante de minha realidade financeira, mas muito íntimo de meus desejos e paixões. Eu não tive dúvidas de que seria a PUC/SP o palco dessa realização; logo esse desejo se tornou realidade e tive uma das grandes alegrias quando, enfim, fui admitida por esta Instituição.

A PUC/SP me trouxe mais quatro grandes alegrias: meus dois filhos, Davi e Laura, meu orientador, Prof. Dr. Márcio Pugliesi e minha coordenação na Comissão de Direito e Processo Civil na OAB subseção de Santo Amaro. Não é demagogia, mas é o mais sincero sentimento de meu coração. Passei por grandes lutas e obstáculos, pois sou empreendedora e com escritório de advocacia próprio para cuidar, um mestrado para fazer e dois filhos para amamentar, Davi concebido no meu primeiro semestre do mestrado, em dezembro de 2017 e, Laurinha, em agosto de 2018. Imaginam como foi tudo isso? Entre um intervalo e outro de aula, saía para amamentar o Dadá durante 20 minutos, ele que ficava me aguardando no estacionamento da Universidade com meu marido. Depois, quando a Laura nasceu, a babá ficava com ela no corredor da Universidade. Em todo o período de gestação dos meus dois filhos, eu ia e voltava vomitando no carro, sentia muito enjoo. Tive sangramentos pelo estresse com diversas situações, e sofria risco prematuro do parto, mas não faltei um dia sequer; eu ia estudar com uma cinta grossa que me ajudava a manter minha barriga forte.

Quando eu pensei que o mundo fosse desabar, porque estava sem orientador em 2019, Deus me envia o Prof. Dr. Márcio, e, no meio de toda essa turbulência, ele me apresentou a nova sociedade de dados — e eu me apaixonei, com tudo o que ele me ensinou... Criei o projeto LGPD do Brasil para estudo científico, e um cliente (do ramo da tecnologia) do meu escritório se interessou; então comercializei o projeto, vi que eles gostaram e foi um tremendo sucesso. Iniciei então consultorias em todo o país e meu projeto se tornou um programa.

Comecei a falar sobre proteção de dados nas minhas redes sociais, e muitos advogados começaram a me seguir e se interessar pelo assunto.

Desde então, fui convidada pela Diretoria da OAB de Santo Amaro para assumir a coordenação de uma comissão; fui convidada para ser assistente do Prof. Dr. Márcio Pugliesi em suas classes na graduação em direito e no mestrado; tenho sido convidada para ministrar palestras e cursos na Escola Superior de Advocacia de Santo Amaro e em diversas empresas públicas e privadas.

Esta Instituição me acolheu quando eu mais precisei de suporte para a entrega deste trabalho, pois com a chegada da pandemia provocada pelo novo Coronavírus, foi muito enlouquecedor estar em casa com dois bebês e ter paz de espírito para terminar de escrever essa dissertação; tive a contribuição e ajuda de meu marido Leandro Loures dos Santos Baccari, que deixou muitos dias de trabalhar fora para ficar em casa com os nossos filhos para que eu pudesse escrever; à minha mãezinha Maria Lucia Baccari que veio ficar em casa durante a pandemia para me ajudar com meus filhos e fazer comida para mim e para minha família; à minha ajudante do lar, a Dona Teresa, ela que tratou de deixar as limpezas diárias que tinha em outras casas para manter a minha casa em ordem.

Com essa etapa concluída, meus sinceros e amorosos agradecimentos:

Ao meu Deus, meu todo-poderoso sobrenatural, que prometeu que eu entregaria este trabalho com sucesso. Você não falha, Deus, eu nem sei se mereço todo esse amor, mas eu vou te honrar por todos os dias de minha vida.

À Pontifícia Universidade Católica de São Paulo e toda Pro-Reitoria e equipe de atendimento da pós-graduação em Direito. Vocês me acalentaram no momento mais frágil de minha vida.

Ao meu Professor e Amigo Márcio Pugliesi, por toda a parceria que teve comigo durante todos esses anos. Você não foi um orientador, você se tornou parte de minha vida, uma pessoa que realmente faz *jus* ao espírito que tem — todos os seus títulos, professor, não alcançariam

a sua hombridade; se colocarmos na parede, estar com você é azimutal. Eu quero e vou trazer muitas felicidades a você com minha amizade e meu trabalho. A confiança não se compra, Professor. E você a depositou em mim em troca de nada. Estar com você é ímpar.

Ao meu marido e paixão da minha vida, Leandro Loures dos Santos Baccari; você preenche todos os requisitos que um dia peticionei a Deus, você extrapola uma parceria de marido e esposa, com você eu posso ir além.

À minha mãezinha Maria Lucia Baccari, que nunca limitou meus sonhos, mas está comigo, colocando a mão embaixo de mim e me abençoando, falando “vai minha filha”. Você é o puro amor, mãe.

À Dona Teresa, minha auxiliadora do meu lar, que abdicou de ganhar mais dinheiro em suas diárias para cuidar de minha família.

À minha edícula, que me acolheu durante as mais de 16 horas diárias que me ausentei no subsolo de minha casa para concluir este trabalho, sozinha e no silêncio de minha mente barulhenta.

À Diretoria da Ordem dos Advogados do Brasil da Subseção de Santo Amaro, na pessoa da Dra. Lisandra Gonçalves e do Dr. Alexandre Fanti, que me confiaram a Comissão de Direito Civil e Processo Civil, e os mais de 70 advogados que estão em minha equipe de estudos sob meu comando.

À Igreja Universal do Reino de Deus, na pessoa do Pastor Filipe Santos, que me acolheu quando eu cheguei desesperada porque eu não conseguia ter concentração para escrever, orou por mim e acompanhou todas essas etapas até eu chegar aqui, desde o início.

A todos os professores que eu conheci durante toda essa etapa, aos funcionários, aos amigos, aos alunos. Sou extremamente abençoada por ter conhecido a todos nesta combatente jornada do mestrado na PUC/SP.

Em especial aos professores da minha qualificação e banca na qual eu tenho profunda honra pela dedicação em receber meu trabalho e pelo pronto-atendimento tão carinhoso, Profª Dra. Clarice Von Oertzen, Profª Dra. Gabriela Gomes Coelho Ferreira, Profº Dr. Antônio Márcio da

Cunha Guimarães e Profº Dr. Marcelo José Grimone. Meu muito obrigada que levarei por toda a minha vida.

## RESUMO

A sociedade passa por uma transformação digital e acelerada transferência de dados e informações pessoais nos meios eletrônicos; é justamente essa razão que leva a inquietação de como as empresas deverão reagir meio a este cenário de proteção de dados pessoais dos cidadãos no Brasil. A busca pelo poder sobre os dados pessoais é antiga, e este trabalho traz à baila análises de casos como de Hitler e o escândalo da empresa Cambridge Analítica nas eleições do Presidente Donald Trump que foram usados como analogia para explicar sobre os desdobramentos do dano social causado pela falta de procedimentos e boas práticas no tratamento dos dados pessoais. Foi necessário realizar o levantamento dos marcos legais sobre a temática desde seu primeiro registo em 1.710 com o Estatuto da Rainha Ana, e entender sobre o plano de fundo desta Lei Federal no Brasil que tem raízes Europeias; depois da revogação da Diretiva 95 que deu enfoque ao Regulamento Europeu 679 em 2016, todos os países que constituem a União Europeia tiverem que criar legislações sobre a proteção de dados pessoais - requisito para manter as relações internacionais entre os países. Ganhou ênfase nos direitos humanos e fundamentais em razão do caráter da privacidade inerente à pessoa humana, mas em contrapartida, gerou a obrigatoriedade dos prestadores de serviços, que neste trabalho tratará apenas das empresas, em cumprir os novos regramentos da Lei Geral de Proteção de Dados Pessoais – Lei 13.709/2018. Com isso, será necessário nortear e reportar às empresas sobre as suas responsabilidades, publicar um texto que informe exatamente o que elas devem fazer, neste momento, para cumprir a responsabilidade social, transparência com o cliente, colaboradores, fornecedores e parceiros, ou seja, as pessoas qual mantém relação comercial para a manutenção do giro econômico, sobretudo, embutidas de segurança jurídica e tecnológica por meio de um *compliance* pautado em procedimentos.



**Palavras-chave:** Avanço Tecnológico; Proteção de Dados Pessoais; LGPD; *Compliance* na LGPD.

## ABSTRACT

The Society is undergoing a digital transformation and accelerated transfer of data and personal information in electronic media; it is precisely this reason that leads to concerns about how companies should react to this scenario of personal data protection of citizens in Brazil. The search for power over personal data is old, and this work brings to light analyzes of cases such as Hitler and the scandal of the Cambridge Analytic company in the elections of President Donald Trump, which were used as an analogy to explain the consequences of the social damage caused. by the lack of procedures and good practices in the processing of personal data. It was necessary to carry out a survey of the legal frameworks on the subject since its first registration in 1710 with the Queen Anne Statute, and to understand the background of this Federal Law in Brazil, which has European roots; after the repeal of Directive 95, which focused on European Regulation 679 in 2016, all countries that make up the European Union had to create legislation on the protection of personal data - a requirement to maintain international relations between countries. It gained emphasis on human and fundamental rights due to the nature of privacy inherent to the human person, but in return, it generated the obligation of service providers, which in this work will deal only with companies, to comply with the new rules of the General Data Protection Law Personal - Law 13.709/2018. With this, it will be necessary to guide and report to companies about their responsibilities, publish a text that informs exactly what they must do at this time, to comply with social responsibility, transparency with the customer, employees, suppliers and partners, that is, the people with whom it maintains a commercial relationship to maintain the economic turnover, above all, built-in legal and technological security through compliance based on procedures.



**Keywords**: Technological Advancement; Protection of Personal Data; LGPD; LGPD Compliance.

## LISTA DE ILUSTRAÇÕES

Figura 1 : Alusão à invasão de privacidade do General Heleno ..... 85

**SUMÁRIO**

1 INTRODUÇÃO ..... 13

1 O PODER E O CONTROLE DOS DADOS PESSOAIS ..... 17

1.1 O Dano Social ..... 24

1.2 Por Que o Controle Deve Ser Controlado, Supervisionado e Ter Regras? ..... 35

2 O NASCIMENTO DA LGPD NO BRASIL E SUA INFLUÊNCIA EUROPEIA ..... 47

3 COMO AS EMPRESAS DEVEM REAGIR À NOVA SOCIEDADE DE DADOS? ..... 84

3.1 O Futuro da Tecnologia a Serviço da Proteção de Dados Pessoais ..... 103

3.2 Mudando a Cultura da Empresa ..... 109

3.3 “Protocolo LGPD-BR”: Como Preparar o Ambiente Corporativo para a recepção da LGPD? ..... 117

3.3.1. Palestra inicial ..... 126

3.3.2. Identificação do cenário ..... 126

3.3.3. Verificação de Vulnerabilidades Sistêmicas (*Pentest*) ..... 126

3.3.4. Criação e Inauguração do Setor de Controle ..... 127

3.3.5. Análise do Perfil do DPO ..... 127

3.3.6. Criação e Inauguração do Canal do Titular de Dados ..... 127

3.3.7. Mapeamento do Fluxo dos Dados (Entrevistas e *Scan*) ..... 128

3.3.8. Análise de Processos e Tecnologias ..... 129

3.3.9. Avaliação do Modelo Atual da Empresa ..... 130

3.3.10. Atualização ou Confecção dos Termos e Políticas de Privacidade Externa (Sites) ..... 130

3.3.11. Atualização ou Confecções de Contratos, Políticas Internas, Código de Ética dos Algoritmos e Regulamento Interno, Acordos Comerciais e Termo de Sigilo e Confidencialidade (NDA).....131
3.3.12. Treinamentos com a Equipe.....132
3.3.13. Realização de Campanhas de Conscientização.....132
3.3.14. Oferecimento de Suporte no Relacionamento com Clientes e com a Autoridade Nacional de Proteção de Dados (ANPD).....133
3.3.15. Início da Pesquisa de Satisfação.....133

CONCLUSÃO ..... 134

REFERÊNCIAS BIBLIOGRÁFICAS.....135

FILMES.....143

# 1 INTRODUÇÃO

O presente trabalho nasceu do interesse nos estudos realizados na matéria de Direito Eletrônico e sua Emergência da Sociedade de Dados, concentrado na proteção de dados com o Filósofo e Professor Doutor Márcio Pugliesi nesta Pós-Graduação *stricto* senso ─ Mestrado em Filosofia do Direito desta renomada Universidade que é a Pontifícia Universidade Católica (PUC) de São Paulo.

Esta Autora analisará a forma, o desenvolvimento, as consequências do tratamento de dados e trará um protocolo de adequação chamado de "Programa de *Compliance* LGPD do Brasil" frente à responsabilidade social das empresas na atual sociedade de dados, já que o Brasil adotou uma legislação específica que trata do tema: a Lei Geral de Proteção de Dados Pessoais – Lei 13.709/2018.

No decorrer da história, o Direito não acompanhou e não conseguiu regular as relações e controles necessários para operacionalizar a tecnologia, e com o seu avanço acelerado, principalmente na pós-industrialização, as relações humanas e o constante uso de aparelhos eletrônicos com transmissão de muitos dados, ganhou destaque e mereceu atenção.

A velocidade com que os dados e informações trafegam e se comunicam de maneira interfronteiriça modificou as formas de convivência social pela praticidade e o tempo economizados, passando tudo a dizer respeito mais sobre conexões de internet e menos sobre as relações pessoais, sobretudo, as físicas.

A pandemia causada pelo novo Coronavírus (SARS-Cov-02), popularmente conhecida como COVID-19, acelerou o processo natural dessas relações, e fez o mundo inteiro ficar conectado instantaneamente para saber de novas informações e atualizações sobre o vírus, a sua rastreabilidade, sua magnitude e avanço pelo mundo; tudo por meio de dados sensíveis, identificando informações essenciais para o combate da doença respiratória aguda que assustou o mundo e a autoridade máxima em saúde ─ a Organização Mundial de Saúde.

As pessoas se viram em total isolamento social e foram compelidas a manter as relações sociais, profissionais, acadêmicas e privadas, em relações puramente virtuais, e as atividades rotineiras se tornando *bytes* e mais *bytes*, antecipando a aceleração dessas relações, já antevista por filósofos.

As memórias de atividades produzidas *face to face* foram reduzidas a lembranças de produção física e, então, a dependência pela máquina ganhou destaque. Neste período, a inteligência artificial tomou força e a busca pelo acesso de dados e informações despertou um olhar diferente sobre muita coisa.

Os dados ganharam valor ─ valor inestimável que durante uma pandemia foram capazes de transmitir informações às pessoas sobre a aproximação do vírus quanto à geolocalização e quanto aos cuidados redobrados; inclusive, o Estado de São Paulo foi o primeiro a divulgar a publicidade sobre a proteção de dados e a fazer uma parceria com as redes de telefonia móvel no que diz respeito ao compartilhamento de dados pessoais para a transmissão de comunicados sobre o vírus[1]. No entanto, durante este período não foi veiculada qualquer publicidade a respeito dos cuidados inerentes a esse compartilhamento de dados, uma vez que o Poder Público também deve assumir responsabilidades quanto aos dados e a sua proteção, até porque é o principal alvo de *crackers* em comparação ao setor privado.

Tempos sombrios em que se insta a extrema necessidade de transmitir informação adequada às empresas para que se possa dar a devida atenção ao tema e tratar os dados pessoais de forma correta, conforme orientação normativa, neste período de *vacatio legis,* quanto às eventuais sanções.

---

[1] TERRA. **Vivo e Governo de SP firmam acordo para controle da COVID-19**. Disponível : https://www.terra.com.br/noticias/coronavirus/vivo-e-governo-de-sp-firmam-acordo-para-controle-da-covid-19,133b7dcece13c62e128b6f6c361c75bc0ftrctgm.html, acesso em 16/06/2021.

Em meio à pandemia, o mundo vive uma guerra virtual ou uma guerra biológica, quem há de acertar essa pergunta? É certo se afirmar que os operadores de Direito precisam serem norteados de como agirem e as empresas receberem educação de uma nova cultura quanto ao tratamento de dados pessoais para que esta terrível situação econômica não se enterre ainda mais, com possíveis penas a serem aplicadas pela Autoridade Nacional de Proteção de Dados.

É preciso divulgar às empresas acerca do nascimento da Lei Geral de Dados Pessoais no Brasil e mapear com informações claras o que é necessário mudar ou implementar para que elas atinjam a finalidade da Lei e respeitem o cidadão com o devido atendimento no que concerne aos dados pessoais e informações que são concebidas por meio desses dados.

Ao final deste trabalho, será possível ter uma visão crítica que se o silêncio imperar sobre o correto tratamento de dados e informações pessoais, as empresas estarão fadadas à falência e ao descrédito. É necessário que haja movimentação prévia dos operadores de Direito que têm papel fundamental na responsabilidade social do país e devem agir com coragem informando e ajudando as empresas nesta adequação; mas para que isso ocorra, as empresas precisam ter o conhecimento da importância deste *compliance*, mesmo que elas não sejam penalizadas, nesse momento, de uma forma mais severa que a Lei impõe por meio das infrações. E, para que este profissional possa contribuir com sua parcela de obrigação moral e ética na sociedade, precisa saber exatamente quais os pontos de transformação são necessários para que as empresas mudem a cultura interna quando o assunto for dados pessoais, entendendo os quatro pilares fundamentais para o procedimento: consultoria jurídica e de cibersegurança; implementação do programa de adequação, que contém 24 fases que compõem a rota de *compliance* – palestra, identificação do cenário, verificação de vulnerabilidades sistêmicas, criação do setor de controle, análise do perfil dos candidatos, inauguração do canal do titular, mapeamento do fluxo de dados pessoais, análise de processos e tecnologias, avaliação

do modelo atual da empresa, revisão dos Termos e Políticas de Privacidade, avaliação de processos e gerenciamento de incidentes e violações, recomendações sobre gaps, emissão de relatório técnico em processos tecnológicos com validações e planos de recomendações, atualizações de contratos, atualizações de políticas internas, códigos de ética e regulamento empresarial, treinamento com a equipe, rodagem de campanhas de conscientização, suporte no relacionamento com cliente e Autoridade Nacional de Proteção de Dados Pessoais, indicação e acompanhamento de *pentest*[2], apontamentos de melhorias de impacto, gerenciamento de novos incidentes/ violações e vulnerabilidades sistêmicas, indicação de seguro de responsabilidade, gestão de resolução de conflitos, pesquisas de satisfação, e; assistência jurídica e administração do programa.

[2] O *pentest* é um teste de intrusão, normalmente realizado por um profissional especializado em segurança cibernética que verifica as condições de vulnerabilidades sistêmicas de determinada máquina nas camadas externas e internas. Existe três estilos: *black-box, grey-box* e *White-box*.

# 1 O PODER E O CONTROLE DOS DADOS PESSOAIS

A busca pelo poder sempre foi pretensão do ser humano que já é acostumado pelo próprio instinto a ter controle e domínio sobre as coisas conforme já se pode ver na Bíblia, mais especificadamente em Gênesis, quando do nascimento de Adão e Eva.

Bastou o Criador dizer que uma única árvore do conhecimento do bem e do mal não poderia ser tocada por eles, ou seja, que eles não teriam domínio sobre aquele fruto, e então, a curiosidade, o *animus* para que pudessem controlar o que estava fora de seus alcances, tocou profundamente a alma de Adão e Eva e acabaram por desrespeitar a ordem de Deus.

> Antes mesmos de serem criados, eles já possuíam domínio[3] sobre o Jardim do Éden, sobre os animais, sobre a água, a terra, as plantas e outros frutos, tudo o que era extremamente necessário para a vivência naquela época; mas a inquietação por algo que fugia da regra estabelecida tomou por completo a consciência de Adão e Eva, que acabaram por não obedecer ao que havia sido imposto, porque naquele momento, por instinto, já queriam ter acesso ao conhecimento.

Veja-se que, saber sobre algo do qual eles não tinham ideia era fundamental para continuar uma vida tranquila no paraíso, e essa escolha por optar entre possuir tudo aquilo que haviam recebido ou possuir realmente tudo aquilo que seus olhos possuíam alcance, foi mais forte do que o regramento imposto por Deus — isso se chama gana por poder.

Pois bem, algo que Bertrand de Jouvenel des Ursins[4] tratou de entender foi que na natureza do poder sempre há uma carga egoística:

---

[3] Gênesis 1:26 E disse Deus: Façamos o homem à nossa imagem, conforme a nossa semelhança; e domine sobre os peixes do mar, e sobre as aves dos céus, e sobre o gado, e sobre toda a terra, e sobre todo o réptil que se move sobre a terra (DANTAS, Maria Augusta. Bíblia Revisitada para Jovens. Campinas: Bookseller, 2020).

[4] Apud STRAUSS, Leo. Direito Natural e História. São Paulo: Martins Fontes, 2020.

um poder que se volta para si mesmo[5], e essa busca pelo poder de Adão e Eva trouxe consigo uma violência que é exatamente algo que está ligada ao poder. Após o incidente, Deus esboçou certa violência quando os castigou, e disse a Eva que sua dor seria multiplicada quando estivesse à beira do parto[6] — perceba, a ação e reação do detentor do poder.

A divisão pelo poder do conhecimento entre o bem e o mal trouxe sérias consequências para os primeiros habitantes da Terra, e é exatamente com este texto inicial que se faz necessária a reflexão entre dados pessoais — poder — controle.

Com esta breve analogia, pode-se perceber que a busca pelo poder é instintivamente atinente ao ser humano, que, imbuído de conhecimento, pode traçar uma meta por essa busca racional, ou ainda, essa busca pode não ser percebida por ele mesmo, mas está no seu DNA natural.

Se poder e violência podem quase sempre aparecer juntos, como pensa a filósofa Maria Celeste Cordeiro Leite dos Santos[7], vê-se que é uma grande realidade a desgraça que trouxe dores ao mundo, uma violência permanente da revolta de Deus com o ser humano que buscou o domínio sobre todas as coisas, nisto procurando denotar que, mesmo sem ter uma meta traçada sobre o domínio completo do paraíso, Adão e Eva promoveram o controle sobre o poder do conhecimento porque já era instintivo do próprio ser humano, quando atraídos pelo mal.

A busca pela informação então veio dos primeiros habitantes da Terra e, com ela, a busca pelo controle e pelo poder, essa combinação perigosa de anseios ajuntada com qualquer dado pessoal que seja mais

---

[5] SANTOS, Maria Celeste Cordeiro Leite dos. **Poder Jurídico e Violência Simbólica**. 01ª – São Paulo: Editora Cultural Paulista, 1985, p. 123.

[6] Gênesis 3:16 E à mulher disse: Multiplicarei grandemente a tua dor, e a tua conceição; com dor darás à luz filhos; e o teu desejo será para o teu marido, e ele te dominará (DOWNEY, Roma; BURNETT, Mark. A BÍBLIA — A História de Deus e Todos Nós. São Paulo: Sextante, 2014, p. 106).

[7] SANTOS, Maria Celeste Cordeiro Leite dos. **Poder Jurídico e Violência Simbólica**. 01ª – São Paulo: Editora Cultural Paulista, 1985.

do que necessário para determinado tratamento, certamente acarretará em sérios danos ao detentor dos dados, caso haja um desrespeito às regras e normas predeterminadas, como foi o caso de Adão e Eva, eles que tiveram uma pena perpétua da desobediência; mas essa alusão ao Direito será tratada mais adiante, no próximo capítulo.

Porque neste capítulo tratar-se-á de alguns dos principais poderosos que tiveram acesso aos dados pessoais e informações que combinaram essa arma perigosa que é o poder com a violência, indo totalmente ao encontro com os estudos da estrutura simbólica do poder de Maria Celeste Cordeiro Leite dos Santos.[8]

Já dizia Platão e Aristóteles que a relação entre o detentor do poder e o cidadão comum não é uma relação entre iguais[9]. Isso significa dizer que, apesar dos dados pessoais serem informações que dizem respeito a pessoa humana, se estes dados estiverem numa base da qual ela não tenha autonomia para acessar o que exatamente tem naquela base, corrigir dados incompletos, inexatos ou desatualizados, ou mesmo pretender a anonimização deles, o bloqueio ou eliminação de dados desnecessários ou excessivos ao que realmente importaria para estar naquela base, haverá prejuízo; utilizar a base para transferir a outro lugar ou até mesmo eliminar, apagar os dados daquele cadastro ─ como é que ela terá direito a todas essas ações entre empresa-cidadão?; esta não é uma relação entre iguais+.

Levantada a questão de que o poder é instintivo do ser humano, traz-se à baila que desde os primórdios os dados pessoais ficam na base do controlador, e este controlador sendo o Estado, de maneira geral, é algo perigoso. Nota-se que na Idade Média usaram deste poder e controle das informações para caçar mulheres que levantassem suspeitas de que praticavam bruxaria ou magias, devendo ser queimadas na fogueira.

---

[8] Idem.

[9] Idem, p. 124.

Se os rituais eram praticados quando não se via, como é que o Estado, por meio da Igreja Católica, teve conhecimento de que certa mulher, em certo endereço, deveria ser queimada e morta pela prática de bruxaria?

Aqui não se procura explicar o motivo pelo qual motivou os católicos a levar essas mulheres à fogueira[10], mas sim, o fato de que eles detinham o controle sobre a religião daquelas mulheres, dado pessoal considerado sensível[11] pela Lei Geral de Dados Pessoais, que hoje deve ser protegido de forma mais segura e com acesso restrito somente às pessoas que necessitam ter acesso à esse dado, justamente porque se deve preservar certos dados que, apenas por sua escolha, poderiam causar consequências adversas. Por isso esse tipo de dado foi considerado ter tratamento especial.

O que se viu ─ também outro grande fato histórico demarcado por terror e muito sangue ─, foram pessoas cuja convicção religiosa ou filiação à organização de caráter religioso, dado referente à saúde, a opção sexual, nacionalidade, e opinião política ou filiação à organização de caráter político foram violentamente procurados pelo exército de Adolf Hitler para marchar direto ao Holocausto.

Hitler tinha os seus ideais que o levaram a criar um modelo perfeito de ser humano, no qual deveria ser belo e para ter a nacionalidade alemã, não bastava ser alemã, a raça, segundo ele, deveria ser pura, e não poderia ter qualquer caráter de dados pessoais que fugissem do esperado por ele.

Percebe-se que entre as pessoas perseguidas e mortas por Hitler estavam os deficientes físicos, aqueles que apresentavam problema de saúde mental, os homossexuais, os que eram contrários ao

---

[10] INSITORIS, Heinrich. O Martelo das Feiticeiras: Malleus Maleficarum, 17ª ed., Introdução histórica: Rose Marie Muraro, Prefácio: Carlos Byington, Tradução Paulo Fróes, Rio de Janeiro: Rosa dos Tempos, 2004.

[11] Art. 5º *Para os fins desta Lei, considera-se: [...]*
*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. [...]*

partido nazista fundado por ele, os ciganos, as testemunhas de Jeová e os famosos judeus[12], ou seja, caros leitores, o líder do nazismo estava tolhendo vidas de pessoas que, hoje, têm os seus dados pessoais sendo considerados sensíveis.

Os dados pessoais eram colhidos por meio do estado, que, em meio ao início dessa Guerra Mundial, que já era uma guerra entre civis que ocupavam a Alemanha, Hitler almejando exterminar essas pessoas determinadas, começou a dificultar a sua vida na sociedade civil, aprovando a Lei para Restauração do Serviço Público Profissional em 7 de abril de 1933, Lei esta que proibia judeus de concorrerem a cargos públicos; após essa primeira Lei, Hitler foi embaraçando a vida dos judeus, quando os proibiu de trabalhar como médicos e advogados.

A pretensão do nazista estava prestes a tornar os judeus como pessoas sem nacionalidade, e a partir de então, outras Leis surgiram como a de Nuremberg e a Noite dos Cristais que deu a inicialização das prisões dos judeus, que seriam mais tarde os principais integrantes dos campos de concentração e extermínio da raça que não era considerada pura. O resto da história gerou a Segunda Guerra Mundial, na qual este trabalho não abordará essa questão.

Marchando mais adiante, já em 2014, outro evento de poder e violência envolvendo dados pessoais foi visto pelo mundo quando aconteceu o escândalo da empresa Cambrigde Analytica[13].

Em um dos casos mais famosos e de grande repercussão, a Cambridge Analytica analisava os dados pessoais e as informações que os cidadãos americanos postavam em suas redes sociais de entretenimento e comunicação entre amigos para manipular as eleições. Mas não era apenas uma simples análise, como relatam os ex-

---

[12] NEVES, Daniel. Holocausto. Disponível em: https://brasilescola.uol.com.br/historiag/holocausto.htm. Último acesso em 12/08/2020.

[13] PRIVACIDADE HACKEADA. Filme, 2019. Disponível em:<https://www.netflix.com/br/title/80117542>. Acesso em 07/2019.

funcionários da empresa, esses dados trabalhavam a favor da campanha de Donald Trump que disputava o cargo de Presidente com a Hillary Clinton em 2016.

Como afirma o jornal BBC, nesta campanha não houve a amostra de diversidade de pensamentos políticos para os indivíduos nas redes sociais, isso significa entender que as pessoas tendenciosas a votar em Donald Trump já tinham o perfil traçado de suas escolhas políticas e, para eles, era mostrado apenas as visões a favor do então, na época, candidato a Presidente Donald Trump; se esse grupo de pessoas fosse a favor dele, ou ainda, que, estivesse em dúvida de quem votaria, acabaria optando por ele.

As análises de perfis e de predição da inteligência artificial produzida por poderosos algoritmos são altamente capazes de entender como funciona o pensamento do indivíduo porque analisou vários dados e informações postadas em redes sociais por um certo período de tempo, tendo condições de mostrar preferências por músicas, tempo de vídeos mais atrativos com a temática que mais lhe agrada; pessoas que mais interage com o quê, tempo de conversas, linguagem e forma de comunicação que é feita pela escrita, pelas curtidas, pelos direcionamentos, e até pelos *emojis* utilizados nas conversas; tempo de expectativa de resposta nas ações que lhes são marcadas etc.

Imagina-se que esse algoritmo é capaz de indicar emoções e até predizer qual seria uma escolha ou uma ação de um indivíduo a uma atividade futura, isso porque a inteligência artificial calcula exatamente qual a chance do indivíduo tomar decisões com base em suas escolhas passadas e presentes. Todo histórico é armazenado pelo *hardware*, reduzindo o conjunto semântico-pragmático do indivíduo a uma série de combinações matemáticas.

O controle pelo poder passou a se tornar o projeto mais ambicioso do indivíduo, porque, como afirma o filósofo Márcio Pugliesi, o homem foi liberto do medo e do mito[14], com o conhecimento mais

[14] PUGLIESI, Márcio. ***Filosofia Geral e do Direito****: uma abordagem sistêmico-construcionista.* Chisinau: Novas Edições Acadêmicas, 2021.

aprimorado da ciência e tecnologia, pôde fazer leituras em massa dos pensamentos dos indivíduos apenas com a manipulação de dados pessoais, por isso, ele denomina a atual sociedade como sendo sociedade de dados ou sociedade de ócios, como tentativa de explicar que as novas tecnologias, que ele inclui a informática, robótica, telemática, inteligência artificial e inteligência artificial distribuída, determinarão para que a produção da mão-de-obra braçal e intelectual do homem terão pequeniníssima contribuição, porque o sistema já estará preparado para trabalhar sozinho.

O sistema será alimentado pelos dados e informações fornecidas pelo próprio indivíduo com ação completamente consciente de publicizá-los, mas talvez, inconscientemente alienados pela sociedade de controle.

A inteligência artificial deu vida àquele desejo do indivíduo de se dedicar ao que lhe faz feliz, e gastar menos tempo com mão de obra porque todo esse trabalho já foi transferido à robótica e aos algoritmos, agindo ele como, se a partir daí, passasse a ter mais controle sobre a sua vida privada e as suas escolhas, no seu agir, no seu pensar e no seu falar, porque todas essas iniciativas partiriam dele, e de suas decisões. Ledo engano.

Uma vez que o indivíduo cria códigos que permitam que o trabalho humano se torne ócio, e menos dependente das máquinas, ele se torna controlado pela tecnologia e por todo engajamento que ela é capaz de infiltrar.

Enquanto cientistas de dados desenvolvem algoritmos que reduzam o trabalho humano, para lhes beneficiarem e contribuírem com o desenvolvimento progressivo da sociedade, outros profissionais da tecnologia utilizam-se destes códigos e fontes abertas para fazer verdadeira leitura do ser humano que virou o produto mais poderoso da face da Terra.

Seres humanos querem controlar seres humanos, mas já parou para pensar que eles caíram numa própria cilada, acreditando eles que

iriam usufruir de benesses criadas por eles próprios pelo medo do trabalho-escravo, talvez pela própria história da cultura escravidão, reflexão acertada do filósofo Márcio Pugliesi: no trabalho, o homem torna-se prisioneiro do seu metabolismo, prende-se à sua condição natural sem jamais transcendê-la, sem se libertar da recorrência cíclica do seu próprio funcionamento[15].

Mas, enquanto isso, o pequeno cérebro de pessoas poderosas controla um exército de dados e informações para enriquecer cada vez mais os seus cofres e perpetuarem-se na instância do poder.

O poder da sociedade de dados está intrinsecamente ligado àquele que detém o controle dos dados pessoais, por isso, o termo determinado por ele de sociedade de controle; o indivíduo que sabe dessas informações se permite viver no controle de sua vida pelo limite que impõe ao uso desta tecnologia que lhe serve, e não permite que se torne a sua senhora ─ quem tem mais informação tem mais poder.

## 1.1 O Dano Social

O dano social é aumentado pelo uso exagerado e descontrolado das novas tecnologias, pelos serviços robóticos e da inteligência artificial, porque com o tempo mais livre, o profissional da engenharia de dados, vivendo na sociedade do ócio, criará, inovará e aperfeiçoará tecnologias existentes, o que resultará numa violência acelerada da humanidade nos meios telemáticos, caso não haja além da normatização, a fiscalização, e a conscientização das boas práticas e ética.

O uso da internet e dos equipamentos eletrônicos já é realidade em todo o mundo, inclusive nas classes sociais mais abastadas essa atividade proporciona uma veiculação gigantesca de informações e processamento de dados em que o mundo do direito ainda não está preparado para recepcionar tal acontecimento.

---

[15] PUGLIESI, Márcio. ***Filosofia Geral e do Direito****: uma abordagem sistêmico-construcionista.* Chisinau: Novas Edições Acadêmicas, 2021, p. 605.

Isso ocorre porque o ser humano não foi preparado para pensar como poderia recepcionar a tecnologia, mas tão somente para criá-la e usá-la. Daí pensariam depois em solucionar conflitos sobre os seus efeitos, pois não imaginaram o dano social que essa falta de controle pudesse causar na sociedade e na humanidade.

Quando se fala no dano social em decorrência do uso da tecnologia acelerada e descontrolada, existem vários impactos negativos a resultar na sociedade, uma vez que se inicia pela diminuição do trabalho do homem, e na consequente diminuição da oferta de emprego, como resultado do empobrecimento de vários indivíduos e aumento da miséria e fome.

A massificação do uso da tecnologia em troca da mão de obra resultou numa diminuição de profissões e na extinção do trabalho braçal, mas para o filósofo Márcio Pugliesi esse fator deve ter sua extrema máxima reportada de preocupação porque é um grave atentado à personalidade[16].

O uso de tecnologias não apenas substituirá os indivíduos de seus postos de trabalho, mas obrigarão pessoas a se ambientarem e a especializarem-se em utilizar desses recursos para aprimoramento do trabalho e como meio, inclusive, de encurtamento de tempo para atingir o aumento das demandas, e proporcionarem mais lucros às empresas.

Esse trabalho com tecnologias de alto desenvolvimento atinge todos os campos e segmentos, tratando e processando muitas informações, gerando um conflito social no que diz respeito à privacidade, intimidade, honra e a todos os direitos inerentes à personalidade humana que são capazes de perturbar a ordem social, como era da preocupação de Émile Durkeim[17].

---

[16] PUGLIESI, Márcio. ***Filosofia Geral e do Direito****: uma abordagem sistêmico-construcionista.* Chisinau: Novas Edições Acadêmicas, 2021, pg. 681.

[17] Apud MEZZETI, Luca; CÉZ, Joaquim Portes Cerqueira. **O Direito das Novas Tecnologias e o Ordenamento Constitucional**. Editora D'Plácido, 2019, p. 29.

Certamente a ordem social está sendo impactada pelo atropelamento do progresso que promove a criação de novas tecnologias, sistemas, deixando e tornando as Leis inatingíveis para se alcançar êxito quanto aos controles e sanções das proteções de dados pessoais.

O grande tráfego de dados e informações pessoais que são geradas nas redes todos os dias estão sendo lidos e assistidos pela inteligência artificial que controla e faz o tratamento dessas operações, armazenando em grandes *datas centers* que, em conjunto com outras empresas recebem e/ou transferem esses dados e informações pessoais, gerando um *big data*.

O algoritmo conhece mais o indivíduo do que ele próprio, capaz de predizer suas escolhas, suas emoções, e suas ações com relação a todos os atos civilizatórios da vida humana. Acontece que se chega a certo ponto em que a inteligência desta inteligência artificial começa a aprender com toda informação que recebe, e como o armazenamento de dados e informações pessoais é muito grande, pelo histórico e período em que o indivíduo tem relacionamento com certa empresa, o sistema de predição que antes era algo assustador se tornou comum, e a *deep learning*, potencialmente ameaçadora para o convívio social humano, mostra-se capaz de destruir a paz e a ordem social.

Quando se passa deste limite entre ações humanas e produção unilateral de máquinas, baseadas no instinto humano de determinar ao indivíduo que ela foi treinada para ser exponencialmente igual, começa-se a gerar conteúdos sozinha, ou seja, a máquina gera conteúdo no lugar de cada qual, mas pelo qual o indivíduo-alvo não fez parte.

Quando se tem um aprendizado como este, a máquina também é capaz de ter uma ação própria e lançar nas redes sociais, por exemplo, um pensamento do qual se gerou sem ação humana e supervisão humana. O problema de tudo isso é que essa máquina não trará rastreabilidade se não for supervisionada, podendo disseminar *fake*

*news*, caso que já vem ocorrendo, principalmente nos Estados Unidos, como foi o caso “Pizzagate”[18].

O “Pizzagate” foi uma teoria da conspiração disseminada por pessoas reais, inclusive celebridades e artistas, em 2016, quando da eleição entre o atual Presidente Donald Trump e a candidata na época Hillary Klinton; acreditou-se que as informações seriam verdadeiras, defendendo esta causa, mas mal sabiam que essa teoria havia sido produzida pela inteligência artificial da *deep learning*, e que tinha como base a *fake news* a atrapalhar as campanhas políticas que ocorreram no mesmo ano.

O grupo WikiLeaks divulgou *e-mails* secretos de Jhon Podesta, líder que tomava conta das campanhas políticas da candidata Hillary Klinton, na qual membros de grupos de discussões anônimos resolveram pesquisar sobre o então conteúdo, e encontraram diversas vezes nos documentos a palavras “queijo” e “pizza”, que foi atrelado ao termo pornografia infantil.

Enquanto a *fake news* foi se espalhando pelas redes sociais, a pizzaria Comet Ping Pong foi ganhando *haters* que acreditavam que naquele estabelecimento comercial havia um porão onde indivíduos pedófilos abusavam de crianças.

Conquanto que o caso fosse totalmente inverídico, ao alcance dos olhos e das mãos de milhares de pessoas, sem fronteiras, e sem qualquer verificação do que era disseminado, grupos começaram a se formar acreditando que realmente haviam pedófilos no porão da pizzaria, até que um dia, um indivíduo desequilibrado pretendeu fazer justiça com as próprias mãos e se dirigiu armado até o estabelecimento (Pizzaria), pronto para salvar as possíveis crianças que estariam sendo abusadas sexualmente. Neste cenário, apesar de Edgar Welch[19] ter disparado por

---

[18] PRIVACIDADE HACKEADA. Filme, 2019. Disponível em:<https://www.netflix.com/br/title/80117542>, com acesso em 07/2019.

[19] REVISTA ABRIL. 2020. **Escândalo da Teoria da Conspiração Pizzagate**. Disponível em: <https://super.abril.com.br/mundo-estranho/pizzagate-o-escandalo-de-fake-news-que-abalou-a-campanha-de-hillary/>, com acesso em 17/09/2020.

três vezes a arma, ninguém saiu ferido pela interferência preliminar da polícia.

Em que pese a internet ter se tornado democrática, o uso indiscriminado atrelado à quantidade de informações circulantes e sem a verificação antecedente do que vem a ser lançado na rede é um grande risco para a sociedade.

O principal risco social que será tratado por este trabalho, para que se mude a cultura do tratamento, armazenamento e proteção desses dados e informações. Exatamente porque o indivíduo é hoje considerado um *citoyen pensè* (cidadão pensado) e não mais um *citoyen penseur* (cidadão pensante)[20], como entende Michel-Lois Rouquete, pois a inteligência artificial preditiva é capaz de pensar o que o indivíduo faria em determinada situação e escolher a opção que mais se aproxima com as últimas ações em que ele teve, com base nos dados que lhe foram alimentados, ou que o algoritmo esteja acompanhando.

O comportamento do ser humano é previsível pelas sensações e linguagens corporais em que ele emana ao ser analisado por outro ser humano. A inteligência artificial consegue fazer verificações em alta escala porque possui mais informações armazenadas em seu *hardware* do que o cérebro humano é capaz de armazenar.

Isso significa dizer, que mesmo se o indivíduo estiver sozinho, mas conectado a um aparelho eletrônico, e principalmente à internet, mesmo que ninguém aparentemente veja o que se esteja fazendo, suas ações serão previsíveis e uma empresa poderá colher e entender como funciona a mente e as ações desta pessoa.

A vida privada realmente se tornou pública, pública para empresas que coletam dados e informações pessoais das quais você não sabe como são armazenadas, quais dados efetivamente são coletados, o que elas fazem com esses dados e informações pessoais, como são tratados, de fato, como por exemplo, onde ficam armazenados, por

---

[20] MEZZETI, Luca; CÉZ, Joaquim Portes Cerqueira. **O Direito das Novas Tecnologias e o Ordenamento Constitucional**. Editora D'Plácido, 2019, p. 29.

quanto tempo salvam, quem tem acesso, com quem compartilham, qual a finalidade que utilizarão seus dados e informações pessoais, qual é espaço que esses dados e informações pessoais ocupam, como ficam quando se transformam em equações e combinações matemáticas e principalmente, qual a conclusão que a seu comportamento teve de determinada situação: a aprovação, desaprovação, qual é a categoria ou denominação que esta empresa utiliza quando se trata de você; porque por mais anonimizado que o seu nome esteja, é possível fazer o caminho reverso e descobrir qual a pessoa física que representava este número. Outra pergunta a ser analisada é se após criarem um perfil para o indivíduo, ele continua a ser monitorado, se além da coleta e monitoramento, existem experimentos com o indivíduo para testar novas tecnologias, ou se utilizando das mesmas tecnologias, eles experimentam impulsos humanos quando acionada determinada criação ou ferramenta, porque, desta maneira, conseguirão calcular quais os êxitos lograrão justamente pela maneira de se alcançar este público.

Ainda mais, se após a identificação da personalidade do indivíduo haverá setores que evidenciam e, de fato, separam pessoas que se encaixam no mesmo perfil para receberem estímulos de ferramentas tecnológicas diferentes das demais.

O controlador desses dados e informações pessoais tem acesso ao resultado deste programa de aperfeiçoamento da ferramenta tecnológica, que pode auditar, quantas vezes determinado indivíduo clicou naquela página, qual caminho percorreu, quantas vezes clicou, compartilhou, visualizou, permaneceu lendo ou olhando para aquela figura, especificar datas, horários, em que essa página foi visitada, inclusive, as pesquisas posteriores ou anteriores que levaram este indivíduo a navegar por esta página.

Enquanto a tecnologia puder favorecer o indivíduo, nascem-se ideias capazes de unir o conforto e a simplicidade aos aparelhos eletrônicos que o indivíduo utiliza no dia-a-dia; desse processo entre unir coisas à pessoas por meio de sensores, surgiu o conceito da Internet das Coisas (IdC), e mais conhecido internacionalmente pelo termo

*Internet of Things* (IoT), conceito dado pelo Britânico Kevin Ashton, fundador do *Auto-ID Center of Technology*, que, em 1999 descobriu como conectar coisas ao ser humano por meio de sensores onipresentes quando realizava pesquisas de radiofrequência e tecnologias de sensores[21].

Se a proposta de Steven Jobs era tornar o celular parte do corpo humano, a Internet das Coisas amplia essa proposta, na medida em que há milhares de objetos a rodear o indivíduo; todos eles terão consigo armazenados dados e informações pessoais das quais serão objeto como prova para qualquer ato jurídico futuro, o que haverá muita discussão sobre a sua possibilidade ou não, inclusive como facilitador de provas eletrônicas, servindo até como possíveis testemunhas.

O perigo é iminente da Internet das Coisas, pois mais aparelhos eletrônicos serão armazenados com informações pessoais dos indivíduos e ficarão neles armazenadas — então, quem controlaria a fiscalização da proteção de dados pessoais de quem comprou esses determinados aparelhos?

Parece que a Autoridade Nacional de Proteção de Dados Pessoais terá muito trabalho a fazer, pois a proteção de dados pessoais não está resumida em proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade do indivíduo em razão da atividade de tratamento que envolva bens ou serviços, mas quando a Lei 13.709/2018, a Lei Geral de Proteção de Dados Pessoais, fala que ela se aplica também ao tratamento de dados de indivíduos, deverão ser bem analisados os produtos pelos quais existem tratamentos, pois dados e informações pessoais são armazenadas em *data centers*.

Apesar da Lei Geral de Proteção de Dados Pessoais (LGPD) não trazer a figura do produto como atividade que também envolva tratamento, poderá o produto ser encaixado na segunda parte do inciso II do artigo 3º para se buscar direitos e deveres do operador que comercializada produtos pelos quais fornece esse tipo de

[21] Kevin Ashtom (2020).

armazenamento, pois, desta forma, já deverá este fornecedor se adequar à legislação.

Existem lacunas na LGPD, por isso, mesmo as movimentações políticas certamente foram feitas para que o Presidente da República Jair Bolsonaro sancionasse esta Lei específica; inclusive, no que tange às penalidades, já que existe um dano social causado pelo avanço da tecnologia, pois o direito não acompanhou esta evolução, por isso, a preocupação em informar e divulgar a extrema necessidade de um *compliance* nas empresas, o que será abordado mais adiante.

A comunicação via dispositivo eletrônico e digital tornará ainda mais difícil a percepção de sensações e expressões da linguagem, misturado a um cenário de informações espalhadas por algoritmos das quais não se saberá quem os propagou aquelas informações, pois o *deep learning* proporciona informações das quais são atrativas para o seu perfil, não fazendo a peneira do que é verdadeiro e do que é falso, ou seja, o sistema tecnológico contribui para que o indivíduo seja enganado, porque existem algoritmos neste exato momento analisando o perfil de cada qual, sem o respectivo consentimento provavelmente, ou se houver, é bem provável que não esteja obedecendo alguns dos fundamentos principais para este assunto trazido neste trabalho ─ a inviolabilidade da intimidade, da honra, e da imagem; o respeito à privacidade, pois não coaduna com a escolha do próprio indivíduo em ter controle sobre suas informações, e longe, muito longe de atender ao que preconizam os Direitos Humanos.

A teoria do construcionismo, pela visão do filósofo Márcio Pugliesi, em que a compreensão da realidade social se dá pela ação dos indivíduos com a conjectura da geografia, demográfia e da cultura onde estão inseridos, isso significa entender que, muito do que o indivíduo tem acesso aos meios digitais e eletrônicos são limitados a região onde ele está inserido e será um recorte da cultura qual possui acesso; ou seja, se esses meios de acessão não se tornarem democráticos de forma uniforme, o país terá um dano social na quantidade de informações que aquele indivíduo está inserido, e como a propagação de *fake news* é seis

vezes maior que a notícia verdadeira[22], a porcentagem de que aquele informação numa cidade do interior terá um efeito mais desastroso e alarmante.

Nesta esteira de pensamento, a realidade social é construída pelo meio natural ou social por uma atmosfera semântico-pragmática[23] a partir de sua visita e por seus meios: interpretação, compreensão; invenção, criação, produção, convenção (em conjunto com outras atmosferas semântico-pragmáticas) em estados históricos e sociais a que pertença[24], de todos os símbolos que o indivíduo representa em suas crenças, línguas e filosofias de vida.

O processo de mitigação de dano social ao impacto da chegada da proteção de dados pessoais deve respeitar as pretensões de ações comunicativas daqueles profissionais que irão implementar adequações necessárias nas empresas, deve respeitar acima de qualquer comunicação, antes, quatro características: ser inteligível, ser verdadeiro, ser justo e ser sincero; ou seja, o profissional que será contratado para realizar as adequações necessárias deve se portar com as caraterísticas apontadas por Habermas[25], caso contrário, informará ao emissor de uma forma que não foi clara, fazendo-o entender de uma

---

[22] JORNAL DA RECORD. 2020. [Televisão na semana de 13 a 19 de setembro de 2020].

[23] O filósofo Márcio Pugliesi explica que a atmosfera semântico-pragmática ajuda o indivíduo a construir sentidos, e que o indivíduo já nasce no ambiente em que ele adquirirá determinada linguagem da qual ele iniciará o seu processo tendo como base esta atmosfera do seu núcleo familiar, e então, passa-se a interagir com o mundo de acordo com esses sentidos obtidos na atmosfera dentro deste núcleo familiar, que adquiriu certo repertório de linguagem, e daí este indivíduo passa a ter uma visão de mundo, ofertada pela sociedade em que está envolto.

[24] PUGLIESI, Márcio. ***Filosofia Geral e do Direito****: uma abordagem sistêmico-construcionista.* Chisinau: Novas Edições Acadêmicas, 2021, pg. 681.

[25] HABERMAS, Jurgen. **The Theory of Communicative Action**, v. I — Reason and the Rationalization of Society; vol. II, Lifeworld and System: a critique of functionalist reason; (1987), 152 p.; Towards a communication-concept of rational collective will-formation. A thought-experiment, in Ratio Juris, v. 2/2, julho 1988, p. 144-154, e a lúcida exposição de síntese de obra de WHITE (1995).

.

outra maneira da qual não terá efetividade para a prevenção dos riscos e possivelmente contribuirá para causar danos sociais.

Os profissionais que atuarão no combate ao dano social provocado por este alucinógeno mundo virtual devem evitar meios de comunicação e de linguagem intersubjetivos e expressões implícitas das quais deixará o emissor entender pela comunicação que este profissional pretendeu passar, evitando ao máximo que não se ocorra patologias da comunicação.

Sabe-se que a linguagem é formada em três subsistemas: o verbal, vocal e o gestual, em que o filósofo Márcio Pugliesi afirma que esses três juntos formam a atmosfera semântico-pragmática que propiciam as comunicações interpessoais, e é exatamente neste sentido em que este trabalho busca chamar a atenção dos leitores para que, primeiramente, se tenha um olhar para esta nova filosofia que tenta trazer à sociedade, o filósofo Márcio Pugliesi, na ânsia de que essas diferenças de atmosferas em que os indivíduos estão inseridos possam ter uma troca de discursos claros para se buscar a qualidade de entendimentos com as linguagens de cada um, mesmo que nunca seja perfeito; mas o importante, pensa ele, é manter essa interação, pois é ela quem dá sentido e faz com que o interlocutor entenda e tenha percepções sobre como o ouvinte recebe essa informação.

Os dados e informações pessoais nas mãos de pessoas que não estão capacitadas para recebê-las é o maior de todos os danos sociais, porque simplesmente eles se alastrarão numa determinada empresa. Tem-se que o maior número de vazamentos de dados pessoais acontece dentro de uma empresa, e ocasionada por um colaborador ou ex-colaborador que foi desligado e que, com suas emoções, leva consigo senhas e acessos sigilosos que são aproveitados pois a empresa não trocou tal acesso quando do desligamento, ou mesmo o indivíduo continua na empresa, tem acesso ao sistema de segurança da informação, caminha pelas vulnerabilidades dos sistemas, e abusa desse conhecimento específico para benefício próprio, como por exemplo, se aproveita de senhas especiais para fazer compras com acesso exclusivo

da qual este acesso não seria destinado para este fim particular, cometendo assim, o chamado *cyber crime*.

O colaborador sabe exatamente as fragilidades do sistema, tem acesso a todos os dados e informações pessoais, considerando aqueles dados sensíveis comentados no início deste trabalho, que foram e são alvos constantes de ataques preconceituosos e discriminatórios, gerando violência e derramamento de sangue.

Enquanto nas empresas públicas que constantemente são atacadas por *crackers*[26], normalmente em busca de vantagem financeira, em que comumente pedem em troca dos dados e informações pessoais, milhões em criptomoedas, as mais pedidas são os *bitcoins* pela dificuldade de lastreio, apesar de que, atualmente seu caminho inverso é facilmente descoberto, e a carteira digital que é criptografada e anonimizada deve ser aberta quando solicitada por autoridades judiciárias, para que se busca obstar lavagem de dinheiro[27].

Quando este evento ocorre, normalmente, o *cracker* assina com seu nome ou apelido, apenas por uma letra inicial de seu nome, se torna famoso de certa maneira em seu meio do *cyber* crime, e normalmente expõe dados de celebridades, famosos, e autoridades públicas, como foi o caso que ocorreu no Brasil quando o Detran deixou que mais de 70 milhões de dados fossem vazados, dados estes constantes na Carteira Nacional de Habilitação (CNH) e que foi possível pesquisar no sítio eletrônico do Departamento Estadual de Trânsito do Rio Grande do Norte (Detran) em que o pesquisador obteve acesso a nome completo, número do CPF, número do RG, a data de nascimento, o sexo, a idade, o número da Carteira Nacional de Habilitação, o endereço completo e a sua foto.

Este pesquisador realizou diversas pesquisas no período de três meses, com número gerados aleatoriamente, no entanto, o Detran não conseguiu explicar o motivo do vazamento à obter acesso a rede

---

[26] Base de estudo realizada pelas análises clínicas desenvolvidas na Advocacia Baccari.

[27] Experiência de campo profissional com clientes do escritório de advocacia onde esta mestranda é sócia.

nacional, inclusive dados pessoais de personalidades famosas foram expostas como do Presidente da República Jair Bolsonaro, da apresentadora de televisão Xuxa Meneguel, do cantor sertanejo Wesley "Safadão", do jogador de futebol brasileiro Neymar Jr., que atualmente faz parte do time Paris San Germain – PSG, Eike Batista, entre outros[28].

O dano social em que há de se exaltar aqui são os impedimentos quanto ao exercício dos direitos dos titulares de dados pessoais, o que importa no retardamento do progresso dos direitos conquistados desde 1789, como se passará a demonstrar no próximo capítulo.

## 1.2 Por Que o Controle Deve Ser Controlado, Supervisionado e Ter Regras?

Na atual sociedade em que quem tem acesso aos dados e informações pessoais é quem tem o poder, partindo do ponto de vista da filósofa Maria Celeste Cordeiro dos Santos, o poder é controle[29], há algo extremamente preocupante, pois quem detém esse poder significa dizer que, tem o controle humano, por isso, as pessoas que controlam os dados pessoais precisam ser controladas, supervisionadas e serem submetidas a regras totalmente severas, buscando-se evitar as barbáries cometidas como aquelas citadas neste capítulo 1 – O Poder e o Controle dos Dados Pessoais.

Por isso, a Declaração Universal dos Direitos Humanos foi tão enfática e logo em seu 2º artigo proteger os indivíduos no tocante a qualquer ato atentatório ou discriminante quanto à raça, cor, sexo, língua, religião, opinião política ou qualquer outra, quanto à origem

---

[28] ABPERITOS, 2020. Disponível em: <https://abperitos.com.br/2019/10/09/exclusivo-detran-vaza-dados-pessoais-de-quase-70-milhoes-de-brasileiros/>. Acesso 22/06/2021.

[29] SANTOS, Maria Celeste Cordeiro Leite dos (coord.); ARAÚJO, Marilene (org.). **O Novo Código de Processo Civil Brasileiro, um enigma a ser decifrado**: percepções cognitivas na interpretação da norma. São Paulo: Editora Max Limonad, 2016, p. 59.

nacional ou social, fortuna, nascimento, qualquer outra situação, ou qualquer distinção quanto aos territórios de países diversos.

Mas para que a segurança pessoal seja efetivada, elas precisam antes ser treinadas e seguir a um manual, por isso, a razão deste trabalho, pois conforme pensa esta filósofa:

> O Direito é, em última análise, um instrumento de controle do comportamento; ele vocaciona e dirige o comportamento de seus destinatários, para que conforme em sua conduta ao padrão estabelecido na norma jurídica. Esta é para alguns uma prescrição, um comando, um imperativo, um conselho. Na medida em que se dirige ao controle do comportamento, esse comportamento será executado por um homem, um grupo etc.[30]

Ela ainda explica que existem quatro formas de controlar o comportamento do indivíduo, entre elas deve-se: verificar a adequação do que foi pedido para a pessoa fazer e o que de fato foi feito; se de repente houver alguma adequação a ser feita, porque o controlado não realizou a atividade conforme o que determinou o controlador, esta inadequação deve ser punida; outra maneira como aponta a filósofa é premiar o controlado quando este obedecer o comportamento que lhe foi imposto; e portanto, conclui-se que, se nada das três hipóteses anteriormente mencionadas derem certo, o controlador deve pressionar ou induzir o controlado para que este se comporte como lhe foi ordenado.

Que tomando como base essa linha de raciocínio sobre as relações comunicativas das personalidades e dos sujeitos da LGPD, pode-se concluir que, dentre eles estão, o operador; o controlador; o encarregado; o titular de dados; a Autoridade Nacional de Proteção de Dados Pessoais; o órgão de pesquisa; a empresa pública, privada ou autônomo (pessoa natural) que presta serviços ao titular de dados. E aí, extremamente por essa razão de haver tantos sujeitos envolvidos nesta relação, é que deve haver um sujeito que não seja parte da relação para se auditar, revisar, supervisionar, fiscalizar, premiar, e até incluir medidas punitivas para os indivíduos que transgredirem as regras impostas pela empresa, a fim de o que este núcleo de controle opere

[30] Idem, p. 59.

com efetividade todo o plano do programa de aperfeiçoamento e proteção de dados pessoais desta empresa.

É de rigor que o controlador deste programa seja essencialmente comandado por um líder que tem a formação em direito, pois o operador de direito especializado em proteção de dados pessoais será o único profissional apto a capitanear este barco. Esta equipe, obrigatoriamente, deverá ser composta por outros profissionais de outras áreas, como é de suma importância que haja um profissional especializado em *cyber* segurança – "*Personal CyberSecurity*", pois este profissional graduado em tecnologia da informação é quem testará as vulnerabilidades sistêmicas da empresa. Este profissional é essencial para que haja consonância com o mapeamento de dados e auditoria documental realizada pelo advogado, a customizar o protocolo de "Programa de *compliance* LGPD do Brasil"[31] que melhor se adequará a essa empresa. Outros profissionais também comporão esta equipe, como estagiários em direito, assistentes jurídicos ou administrativo, bacharel em direito, psicanalistas etc. Estes profissionais devem constituir essa equipe macrossistêmica.

Não obstante, o líder dela deverá ser um operador do direito, pois o operador do direito é o profissional que jurou sob a ética do estatuto da advocacia da Ordem dos Advogados do Brasil que defenderia a Constituição Federal, a ordem para que se tenha um estado democrático de direito, que defenderia os direitos humanos, a boa aplicação das Leis, a justiça social; o advogado jurou que seria meio, o instrumento para a rápida administração da justiça e que seria meio para o aperfeiçoamento da cultura e das instituições jurídicas, ou seja, o advogado que é essencial para a justiça. Não poderia ter profissional melhor a ser líder desta operação de inovação da cultura empresarial no que diz respeito a proteção de dados e informações pessoais.

[31] O Programa de Compliance LGPD do Brasil foi criado pela autora, com base nas legislações estudadas neste trabalho. É um protocolo para adequar empresas de pequeno porte à grande porte nesta legislação específica de proteção de dados no Brasil.

O advogado que é figura representativa da Lei, deve sob a moral, a ética e os bons costumes fazer valer os direitos dos indivíduos, por isso, não haveria profissional melhor do que ele para interpretar a Lei Geral de Proteção de Dados Pessoais sobre a base estrutural que é a proteção dos direitos humanos, e então, implementar o programa que atenda efetivamente aos direitos dos indivíduos, estes chamados de titulares pela Lei.

Sendo o advogado o gestor deste programa, promoverá o valor da eficiência e segurança jurídica, institutos denominados por Robert Alexy[32], pois ele conhece os fatos, o valor e a norma; ninguém melhor do que o advogado para aplicar os meios de coerção e obrigação de sua perfeita execução.

A contínua obediência é fator predominante para que alcance a efetividade da eficácia plena trazida pela Lei geral de Proteção de Dados Pessoais, desta maneira, responde o motivo pelo qual o Programa de *Compliance* LGPD do Brasil deve ser constantemente controlado, supervisionado e ter regras.

A reflexão da filósofa Maria Celeste Cordeiro Leite dos Santos encaixa-se como uma luva neste subtítulo pensando nesta nova sociedade de dados e o que se esperar do implementador do programa de *compliance* em proteção de dados pessoais:

> A intensificação da complexidade da sociedade promove novos problemas a serem absorvidos para todas as esferas de sentido e induz a formação de sistemas sociais com fusões e estruturas próprias, capazes de gerir a complexidade social ao especializarem-se em determinado tipo de comunicação.[33]

---

[32] ALEXY, Robert. **Teoria da Argumentação Jurídica**. A Teoria do discurso racional como Teoria da Fundamentação Jurídica. Rio de Janeiro, Forense, 2011, p. 47-49.

[33] SANTOS, Maria Celeste Cordeiro Leite dos (coord.); ARAÚJO, Marilene (org.). **O Novo Código de Processo Civil Brasileiro, um enigma a ser decifrado**: percepções cognitivas na interpretação da norma. São Paulo: Editora Max Limonad, 2016, p. 63.

Essa complexidade da sociedade, em um caminho que seria natural a olhar da inovação e da promoção de novas tecnologias, da intimidade com os aparelhos eletrônicos e digitais se aceleraram com a chegada da pandemia do novo Coronavírus, tornando extremamente pertinente a figura de alguém que controlasse e recepcionasse essa norma às empresas executarem o seu papel de adequação e estruturação própria que promovessem o respeito e os direitos dos indivíduos, assegurando a boa-fé e os princípios da finalidade, da adequação, da necessidade, do livre acesso, da qualidade dos dados, da transparência, da segurança, da prevenção, da não discriminação, e da responsabilização à prestação de contas aos titulares desses direitos dados pelos agentes de tratamentos dos dados pessoais e das informações atinentes à eles.

O advogado é o mais indicado para ser o gestor deste programa porque no desenho do projeto ele bem entenderá a garantia dos direitos fundamentais de liberdade, de intimidade e de privacidade do indivíduo ao iniciar o processo de mapeamento dos dados pessoais (*assessment*), lastreando, principalmente, os dados pessoais sensíveis estes que provocam o extremo dano social quando estão nas mãos de operadores que não foram previamente treinados e não estão aptos a tratá-los, pelo ponto de vista da segurança e da proteção.

O dado pessoal sensível[34] é aquele denominado pela Lei Geral de Proteção de Dados Pessoais como dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dado referente a saúde ou a vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; e que foi explicado sobre a sua segurança e sigilo em decorrência dos graves acontecimentos históricos com pessoas que

---

[34] **Art. 5º**. *Para os fins desta Lei, considera-se: [...]*

*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. [...]*

estiveram no poder com acesso exclusivo a esses dados que feriram e mataram, derramando sangue inocente por conta exclusiva de optarem, terem ou nascerem com quaisquer destes atributos ou desígnios tido como dado pessoal sensível, por isso, no mapeamento de dados deve-se dar prioridade à eles e daí a extrema atenção quando a empresa tratar dados pessoais sensíveis, justamente pelos acontecimentos passados para que sirvam como péssimo exemplo que esteve nas mãos de pessoas que trataram deles à luz dos direitos humanos.

Sempre que possível, esses dados pessoais sensíveis devem ser anonimizados pelas empresas para a preservação do indivíduo e consequentemente para proteção de sua vida ou da sua incolumidade física ou de terceiros envolvidos.

Sobretudo, este controle deve garantir a transparência entre os atos relacionados, o tratamento de dados pessoais da empresa e o titular de dados para se garantir que o indivíduo tenha acesso ao seu cadastro pessoal, a correção de dados incompletos, errados ou desatualizados, a eliminação de dados não desejados pelo indivíduo ou ainda excessivos, a garantia de que esse cadastro poderá ser repassado para outro órgão ou outra empresa e o seu armazenamento seguro e protegido de possíveis *malwares*, pelo tempo necessário à sua execução do serviço.

A supervisão consiste no suprassumo de se preservar qualquer incitação à discriminação e preconceito, desta forma, os dados sensíveis, que são informações atinentes que podem levar a tal ato discriminatório devem estar seguros, quando for possível a sua anonimização, ou nos casos em que não for possível, e não houver consentimento do indivíduo (titular dos dados pessoais), em razão de cumprimento de obrigação legal ou regulatória pelo controlador; de atos realizados pela administração pública, para realização de estudos de pesquisas, para a execução de contrato ou procedimentos relacionados, em processos judiciais, administrativos ou arbitrários; para a proteção da vida ou incolumidade física do indivíduo ou de outros envolvidos no caso; para algo urgente relacionado da sua saúde, serviços ou de

autoridade sanitária; para atender interesses do controlador ou de um terceiro envolvido no caso; para a proteção do crédito do indivíduo.

O advogado, que aqui neste trabalho é o mais indicado para ser o gestor do Programa de *Compliance LGPD* do Brasil, porque é o profissional mais hábil simultaneamente, em palavras, em gestos, na escrita e na relação com outras pessoas. A formação em direito permite que este profissional, também pela experiência no tratamento e no atendimento geralmente com muitas pessoas, e pessoas diferentes, tende a simplificar todo ato que está ocorrendo para ser o condutor e supervisor da implementação do Programa de *Compliance* em proteção de dados, haja vista, a comunicação com pessoas de todos os tipos de setores existentes numa empresa; mas ao mesmo tempo, o advogado é hábil e técnico para expor mediante relatório claro e completo sobre o mapeamento de dados pessoais e sua finalidade específica utilizada com critérios válidos que lhe garantam a legalidade do exercício deste tratamento de dados pessoais.

Ele é o profissional que mais destaca-se para ser o indicado, além de ter por profissão a advocacia, e importante salientar que o advogado não pode ser parte da empresa na qual vai implementar o "Programa de *Compliance* LGPD do Brasil".

A equipe de tecnologia deste advogado deverá ser contratada pela empresa, de preferência que não tenha profissionais da equipe que trabalhem dentro do ambiente físico da empresa, pois é desejável que esta liderança não seja parte do processo, mas sim, comande o processo, pois neste caso, quando houver de se buscar pela verdade, logicamente para a construção de uma defesa, após a ocorrência de um evento danoso contra a empresa, para assegurar a efetividade desta defesa e na pesquisa da busca pela verdade, a equipe que será externa, terá mais condições de avaliação, porque não se envolveu emocionalmente com quaisquer dos colaboradores da empresa, assim como pensa o filósofo Michel Foucault.

Trata-se de um procedimento que permite a intervenção de um terceiro indivíduo que se coloque entre os dois, como elemento neutro,

procurando a verdade, tentando saber qual dos dois disse a verdade; um procedimento de inquérito, uma pesquisa da verdade nunca intervém em um sistema desse tipo...[35].

Se poder é controle, e quem está no controle possui o saber, este mesmo filósofo entende que, poder e saber encontram-se assim firmemente enraizados; eles não se superpõem às relações de produção, mas se encontram enraizados muito profundamente naquilo que as constitui[36], por mais que pense que este profissional é completo, pois além de toda a representatividade embutida em sua categoria profissional, representar a Lei e ser indispensável pela justiça - o advogado é o detentor do conhecimento de como fazer, executar, supervisionar e defender em caso de incidentes à empresa, acima de tudo, presa pelo respeito aos direitos fundamentais do indivíduo, por isso, é o profissional mais indicado para ocupar este lugar.

Outro ponto de extrema relevância em escolher o advogado para essa difícil missão é porque, de acordo com a teoria do discurso de Habermas[37], o discurso deve ser comunicativo, de uma maneira em que o falante e o ouvinte se entenda, entre o discurso teórico e o discurso prático, assim como o filósofo Márcio Pugliesi pensa, o indivíduo é um ser semântico-pragmático; essa é a condição perfeita de comunicação que até parece reconhecer se o falante tinha a fala sincera, já que em palavras e gestos é possível ter esta percepção; desta maneira o advogado é articulado, requisito imprescindível para ser o meio dessa comunicação.

Após a implementação do "Programa de *Compliance* LGPD do Brasil", faz-se necessário o uso da teoria da argumentação jurídica de Robert Alexy, no que diz respeito ao controle do que já foi executado,

---

[35] FOUCAULT, Michel. **A Verdade e as Formas Jurídicas**. Tradução Eduardo Jardim e Roberto Machado. Rio de Janeiro: Editora Nau, 2013, p. 61.

[36] Idem, p. 123.

[37] ATIENZA, Manuel. **As Razões do Direito – Teorias da Argumentação Jurídica**. Tradução de Maria Cristina Guimarães Cupertino. São Paulo: Landy Editora, 2006, p. 162 e ss.

parece então passar a contínua validade das regras impostas na empresa pelos atos de fala deste comunicador, pois conforme pensa Robert Alex, se não houver fala não haverá forma de comportamento humano esperada para se valer o programa, pois de acordo com ele, a renúncia da fala é renúncia de formas de comportamento humano.

Com todo o exposto, vale trazer as regras fundamentais do discurso prático que defende Robert Alexy que este advogado gestor deverá obedecer aos cinco fundamentos para que o discurso prático quanto aos ensinamentos e supervisão das regras e novos modelos culturais implementados pela empresa para se adequar à nova LGPD. São eles:

> Nenhum falante pode se contradizer.
> Todo falante só pode afirmar aquilo em que ele próprio crê.
> Todo falante que aplique um predicado F a um objeto A, deve estar disposto a aplicar também a qualquer outro objeto igual A, em todos os aspectos relevantes.
> Todo falante só pode afirmar aqueles juízos de valor e de dever que afirmaria também em todas as situações iguais, em todos os aspectos relevantes.
> Falantes diferentes não podem usar a mesma expressão com significados diferentes[38].

Essas brilhantes regras devem compor o cenário de *compliance* que, sobretudo, a depender do porte da empresa, atinge milhares de pessoas, colaboradores e que por conseguinte essas milhares de pessoas terão comunicação com os clientes, que de certa forma precisam ter esse homogêneo conjunto de regras fundamentais para que esse discurso seja limpo e o advogado gestor desta implementação não seja um indivíduo portador da forma de poluição semântico-pragmática (Márcio Pugliesi).

Na mesma esteira de pensamento do filósofo Márcio Pugliesi, conclui-se que este advogado deve possuir uma formação com o *sujeito coletivo* (Márcio Pugliesi) para que ele seja forte o suficiente e

---

[38] ATIENZA, Manuel. **As Razões do Direito – Teorias da Argumentação Jurídica**. Tradução de Maria Cristina Guimarães Cupertino. São Paulo: Landy Editora, 2006, p. 166.

perspicazmente técnico para que a sua linguagem seja clara, acessível e compreendida de toda a poluição semântico-pragmática, porque é muito difícil e para ele, não há como evitar certo grau de ideologia e de variáveis próprias do indivíduo e do grupo[39], por isso, a fala deve ser uníssona.

É de se alertar sobre essa poluição, apenas de ser difícil em manter distante à poluição que acompanha a linguagem do ser humano pelo meio em que se vive ou pelo meio em que se viveu, e pelas pessoas que conheceu, pelas experiências das quais experimentou em determinados ciclos sociais, pois é elementar o acompanhamento desta poluição que enraíza o indivíduo como ser semântico-pragmático.

O filósofo Márcio Pugliesi faz um prospecto sobre a ética como regra de ouro e trazida à este cenário da responsabilidade social das empresas quanto à proteção de dados pessoais, então, a partir daí, pode-se refletir que a responsabilidade social do advogado quanto à aprendizagem dessas novas regras mexe na estrutura da base de governança, privacidade, normatividade, e condutas esperadas (ética) e reguladas pela empresa aos seus subordinados, aos seus colaboradores, aos seus funcionários, aos seus prestadores de serviços, aos fornecedores, aos seus clientes, e é desta forma que deve ser conduzida a regra de ouro que remete a ética: como devo me comportar para produzir o menor prejuízo à todos − essa é uma questão trazida por ele na visão de Žižek, Slavoj.[40.]

É pensando essencialmente nesta pergunta que a alteração no comportamento destes indivíduos deve iniciar para que desde o princípio essas pessoas tenham a ética, o respeito e a reciprocidade ao próximo, respeitando o avanço tecnológico, mas conduzindo o uso desses aparelhos eletrônicos e meios digitais de forma à minimizar prejuízos a empresa, tendo como fundamento a preservação dos direitos humanos relativas aos titulares de direitos dos dados pessoais e é com este

---

[39] PUGLIESI, Márcio. ***Filosofia Geral e do Direito****: uma abordagem sistêmico-construcionista.* Chisinau: Novas Edições Acadêmicas, 2021, p. 736.

[40] Idem, p. 1012.

pensamento que ele por conseguinte contribuirá para que o sistema seja movimentado de forma orgânica, saudável e muito mais abrangente do que a própria legislação.

Deve ser observado pelo advogado o limite entre o que é íntimo, privado e público, respeitando os critérios normativos e fundamentos básicos trazidos pela Lei Geral de Proteção de Dados Pessoais, afastando conforme seja possível o cenário que lhe maquie informações, que restrinja ou proíba de certa forma o seu acesso imediato ao seu cadastro de dados pessoais e informações que lhe dizem respeito.

O dano apontado no item anterior é ilimitado e a sua extensão é totalmente imprevisível porque a era é da sociedade de dados, isso significa dizer que todos os dados pessoais e informações digitais dos indivíduos estão armazenadas em uma *cloud* que pode ser transferida ou compartilhada para milhares de pessoas em cópias fiéis e quase que impossível de serem rastreadas, com o caminho feito quando do compartilhamento dessas telas; por isso, deve-se buscar no profissional, a redução deste dano, pois além de tudo, o que foi visto no passado e ainda é visto no presente, são crimes terríveis ligados à pessoa mas que detêm o poder e controle de dados e informações pessoais, principalmente sensíveis.

Quando o cenário ultrapassa a tortura e chega à morte é impossível trazer de volta ao mesmo cenário para que a situação seja contornada porque ela, é algo irreversível, não há como trazer um indivíduo morto à vida e nessa última *ratio,* propõe-se que seja implementado por completo o “Programa de *Compliance* LGPD do Brasil” para empresas e que a adoção de medidas seja liderada pelo advogado que carregaria essa incumbência. Ele é importante perante a sociedade, tendo inclusive um artigo todo especial na Constituição Federal do Brasil dizendo que o advogado é indispensável à administração da justiça sendo inviolável por seus atos e manifestações no exercício da profissão, nos limites da Lei[41].

[41] Art. 133 da Constituição Federal (VADEMECUM SARAIVA, 2020).

Ao advogado é atribuída essa função e que encerra este capítulo lembrando que:

> O advogado, indispensável à administração da justiça, é defensor do estado democrático de direito, dos direitos humanos e garantias fundamentais, da cidadania, da moralidade da justiça e da paz social cumprindo-lhe exercer o seu Ministério em consonância com a sua elevada função pública e com os valores que lhes são inerentes[42].

[42] Art. 2º do Código de Ética e Disciplina da Ordem dos Advogados do Brasil (VADEMECUM SARAIVA, 2020).

# 2 O NASCIMENTO DA LGPD NO BRASIL E SUA INFLUÊNCIA EUROPEIA

Para se entender o plano de fundo da Lei de Proteção de Dados Pessoais, faz-se necessário entender que desde 1789 se previa o direito de exercer a liberdade, mas com restrições, isso significa entender que, quando a liberdade acaba, inicia a privacidade; observe o texto da lei: A liberdade consiste em poder fazer tudo que não prejudique o próximo, contida no artigo 4º da Declaração de Direitos do Homem e do Cidadão de 26 de agosto de 1789[43].

A Declaração de Direitos do Homem e do Cidadão foi escrita pelos representantes do povo francês em uma Assembleia Nacional, cujo propósito era exaltar os direitos e os deveres Contidos na Constituição e para a Felicidade do povo[44].

Outro artigo que chama atenção é o que trata sobre a religião, pois como será visto mais adiante, a escolha da religião pelo titular de dados é um dado pessoal sensível[45] tratado pela Lei Geral de Proteção de Dados Pessoais − 13.709/2018. O artigo 10º da Declaração de

---

[43] **Art. 4º**. *A liberdade consiste em poder fazer tudo que não prejudique o próximo. Assim, o exercício dos direitos naturais de cada homem não tem por limites senão aqueles que asseguram aos outros membros da sociedade o gozo dos mesmos direitos. Estes limites apenas podem ser determinados pela lei*.

[44] UNIVERSIDADE DE SÃO PAULO, 2020. Biblioteca Virtual de Direitos Humanos. Disponível em: <http://www.direitoshumanos.usp.br/index.php/Documentos-anteriores-%C3%A0-cria%C3%A7%C3%A3o-da-Sociedade-das-Na%C3%A7%C3%B5es-at%C3%A9-1919/declaracao-de-direitos-do-homem-e-do-cidadao-1789.html>, com acesso em 22/09/2020.

[45] **Art. 5º**. *Para os fins desta Lei, considera-se: [...]*

*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. [...]*

Direitos do Domem e do Cidadão[46], do povo francês, aduz que ninguém pode ser molestado por suas opiniões, incluindo opiniões religiosas, desde que sua manifestação não perturbe a ordem pública estabelecida pela Lei. Mesmo que haja na mesma frase uma certa limitação imposta pelo legislador, ao que tudo indica para manter o controle naquela época, a escolha da religião estava entre os 17 direitos e deveres do cidadão francês, o que significa importar com a convicção religiosa, que apesar de não constar como um dado pessoal, já se demonstrava a importância e sua proteção em Lei.

E é neste cenário de liberdade e privacidade que é necessário olhar para 1890, em um artigo publicado na revista de Harvard Law Review, em que Samuel Warren e Louis Brandeis trataram sobre "O Direito à Privacidade". Parece inacreditável saber que esse artigo foi publicado há mais de um século, e que já se exprimia um aborrecimento sobre a invasão da privacidade, assunto trabalhado por William Prosser nos Estados Unidos, do qual contribuiu para tal inspiração[47].

Após esses acontecimentos marcados pela história, que apesar de profundamente tristes, se faziam necessários trazer à reflexão para iniciar o assunto legislativo é de rigor começar pela citação da mãe do direito da proteção de dados pessoais que é a Declaração Universal dos Direitos Humanos – 1948, cujo texto tratou de reconhecer a dignidade humana, proteger liberdades e direitos fundamentais para proteção de direitos civil, políticos, econômicos, sociais e culturais por conta do desrespeito à vida humana e das barbaridades cometidas, ceifando vidas pela opção de crenças, e de dados que são congêneres, pensando no bem da nação e nos estados-membros que dela fazem parte, a Assembleia Geral das Nações Unidas proclamou a Declaração Universal dos Direitos Humanos.

---

[46] **Art. 10º**. *Ninguém pode ser molestado por suas opiniões, incluindo opiniões religiosas, desde que sua manifestação não perturbe a ordem pública estabelecida pela lei.*

[47] Conhecimento adquirido em Aula do Curso de LGPD (Extensão) no "Meu Curso" em janeiro de 2020.

Logo no primeiro artigo[48], o legislador fez questão de mencionar que não existe desigualdade em direitos e as pessoas devem se tratar com espírito da fraternidade, e esse artigo vai totalmente de encontro com a intenção que esse trabalho teve de trazer ao leitor o tocante de que os dirigentes das empresas devem implementar o "Programa de *Compliance* LGPD do Brasil" se colocando no lugar de seus funcionários, colaboradores, clientes, prestadores de serviços e fornecedores, para que busquem medidas das quais eles gostariam de receber quando do tratamento de seus próprios dados pessoais.

A ordem do assunto trazido nesta declaração é bem importante porque faz pensar quais são as prioridades do legislador, veja-se que, no artigo segundo ele já traz proteção dos direitos quanto aos dados pessoais sensíveis cujos são discriminados como raça, cor, sexo, língua, religião, opinião política, origem nacional ou social, riqueza, nascimento, qualquer outra condição que esteja o indivíduo, e neste último trecho pode-se subentender aí condição de saúde, o que não foi expressamente adotado pelo legislador neste artigo.

Fica bem claro que o legislador quis proteger qualquer ato discriminatório e logo de início já optou por proteger os dados pessoais sensíveis, pois é fato que são eles o motivo para a origem do preconceito dispensado a milhares de pessoas no passado.

É visto também a proteção da vida privada, ou seja, a inviolabilidade da intimidade preservando a honra e a reputação da pessoa a ataques que invadam a sua privacidade (art. 12)[49].

Pelos horrores cometidos por Hitler, a Declaração Universal dos Direitos Humano teve de escrever o que na verdade é natural do ser

---

[48] **Art. 1º**. *Todos os seres humanos nascem livres e iguais em dignidade e direitos. São dotados de razão e consciência e devem agir em relação uns aos outros com espírito de fraternidade.*

[49] **Art. 12.** *Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques*.

humano − o direito à sua nacionalidade, isso tudo porque este ditador tinha em sua mente que pessoas de outras nacionalidades que não fossem alemãs, eram inferiores à sua raça e, por isso, deveriam morrer. E que pela nacionalidade não podiam se casar com pessoas da nacionalidade alemã e muito menos ter filhos com elas, eles foram perseguidos até a morte, por isso, esse direito teve de ser escrito no artigo 15[50] da suprarreferida Lei.

Após dois anos, em Roma, em 4/11/1950 foi celebrada a Convenção Europeia de Direitos Humanos, um tratado internacional que reuniu esforços para legislar quanto à proteção dos direitos humanos e das liberdades fundamentais na Europa, logo a garantir os direitos e liberdades sobre a vida, sobre a proibição da tortura, pois, como visto, as violências provocadas advieram das informações contidas nos dados pessoais dos indivíduos.

Assim como na Declaração Universal dos Direitos Humanos, a Convenção Europeia de Direitos Humanos, em seu artigo 08º, trouxe em seu artigo o direito ao respeito pela vida privada e familiar: “qualquer pessoa tem direito ao respeito da sua vida privada e familiar do seu domicílio e da sua correspondência.”

Interessante notar que desde a proteção dos direitos do homem pela convenção francesa, primeiro texto destacado neste título, os próximos textos legislativos seguindo uma ordem cronológica do tempo, também acompanharam essas proteções, que hoje são proteção aos dados pessoais e que são considerados sensíveis; veja que no artigo 9º da Convenção Europeia de Direitos Humanos, a liberdade de religião, ou de crença é preservada, e desta vez o texto prevê a sua manifestação em público e em ordem privada, já ampliando o que se debate.

A proteção de dados sensíveis quanto à discriminação e ao preconceito, ainda sim, continuam sendo destacadas nos textos da

---

[50] **Art. 15**.

*1. Todo ser humano tem direito a uma nacionalidade.*
*2. Ninguém será arbitrariamente privado de sua nacionalidade, nem do direito de mudar de nacionalidade.*

Convenção Europeia de Direitos Humanos e desta vez no artigo 14[51], aduz destaque a proibição de discriminação quanto ao sexo, raça, a cor, a língua, a religião, a opiniões políticas ou outras, a origem nacional ou social, a pertença à riqueza, nascimento ou qualquer outra situação.

Bem, pode-se destacar o artigo 17[52] que trata da proibição do abuso de direito quando existe uma prática que confronte o direito reconhecido na Convenção Europeia de Direitos Humanos quando houver ameaça à proteção dos direitos pessoais destacados por ato discriminatório e preconceituoso, o que significa entender que ali, já em 1950, por mais que não houvesse explicitamente a nomenclatura da proteção de dados pessoais, havia ali o direito do homem quanto à sua identidade e proibição quanto aos atos que o reprimissem a utilização desse direito.

A Convenção Europeia de Direitos Humanos adicionou seu protocolo de número 4, assinado em Paris em 20/03/1952, e que foi adicionado em Estrasburgo em 16/09/1963[53], no artigo 2º[54], também

---

[51] **ART. 14**. ***Proibição de discriminação***. *O gozo dos direitos e liberdades reconhecidos na presente Convenção deve ser assegurado sem quaisquer distinções, tais como as fundadas no sexo, raça, cor, língua, religião, opiniões políticas ou outras, a origem nacional ou social, a pertença a uma minoria nacional, a riqueza, o nascimento ou qualquer outra situação. [grifo nosso]*

[52] **ART. 17**. *Proibição do abuso de direito. Nenhuma das disposições da presente Convenção se pode interpretar no sentido de implicar para um Estado, grupo ou indivíduo qualquer direito de se dedicar a actividade ou praticar actos em ordem à destruição dos direitos ou liberdades reconhecidos na presente Convenção ou a maiores limitações de tais direitos e liberdades do que as previstas na Convenção. [grifo nosso]*

[53] Convenção Europeia de Direitos Humanos. Disponível em: https://echr.coe.int/documents/convention_por.pdf. Acesso: 21/06/2021.

[54] **ART. 2°**. *Liberdade de circulação. 1. Qualquer pessoa que se encontra em situação regular em território de um Estado tem direito a nele circular livremente e a escolher livremente a sua residência. 2. Toda a pessoa é livre de deixar um país qualquer,*

fazendo menção sobre a liberdade da circulação de pessoas de um território por outro, isso significando importar quanto à preservação de um dado pessoal que é a nacionalidade como obstáculo ao não preconceito sobre a sua origem. Bem acrescentada a proibição da expulsão de nacionais, em seu artigo 3º[55].

Não obstante os estados-membros do conselho da Europa acrescentou o protocolo de número 12 implementando uma interdição geral sobre a discriminação. Note que foi necessário dizer novamente o que já havia sido dito em 1950, exaltando novamente o direito de não ser alvo de preconceito a pessoa pela sua raça, pela sua cor, pela língua, pela religião, pelas convicções políticas, pela origem nacional ou social, por um grupo de minoria nacional, pela sua riqueza, pelo seu Nascimento ou outra situação, veja que nos anos de 2000, o legislador reafirmou o artigo 1º do primeiro texto[56].

Como visto no Brasil pelos acontecimentos repetidos, isso em diversas questões sobre a discriminação, e sobre atos que trazem

---

*incluindo o seu próprio. 3. O exercício destes direitos não pode ser objecto de outras restrições senão as que, previstas pela lei, constituem providências necessárias, numa sociedade democrática, para a segurança nacional, a segurança pública, a manutenção da ordem pública, a prevenção de infracções penais, a protecção da saúde ou da moral ou a salvaguarda dos direitos e liberdades de terceiros. 4. Os direitos reconhecidos no parágrafo 1 podem igualmente, em certas zonas determinadas, ser objecto de restrições que, previstas pela lei, se justifiquem pelo interesse público numa sociedade democrática.* [grifo nosso]

[55] **ART. 3°.** ***Proibição da expulsão de nacionais****. 1. Ninguém pode ser expulso, em virtude de disposição individual ou colectiva, do território do Estado de que for cidadão. 2. Ninguém pode ser privado do direito de entrar no território do Estado de que for cidadão.* [grifo nosso]

[56] **ART. 1º.** ***Interdição geral de discriminação****. 1. O gozo de todo e qualquer direito previsto na lei deve ser garantido sem discriminação alguma em razão, nomeadamente, do sexo, raça, cor, língua, religião, convicções políticas ou outras, origem nacional ou social, pertença a uma minoria nacional, riqueza, nascimento ou outra situação.* [grifo nosso]

alguma certa penalidade ao transgressor da Lei, o legislador vê a necessidade de repetir o que já foi dito, isto porque ao que tudo indica, não há eficácia da Lei, até porque, naquele momento não havia a menção de que essas informações mesmo que atinentes à pessoa humana, por mais que sejam explícitas, não estava escrito que é de propriedade delas, assim como foi o caso do que deixou bem claro a Lei Geral de Proteção de Dados Pessoais que até denominou como titular do dado pessoal.

Assinado em Roma, em 25/03/1957, o Tratado sobre o Funcionamento da União Europeia[57] assinado pela majestade, o rei dos belgas, o Presidente da República Federal da Alemanha, o Presidente da República Francesa, o presidente da República Italiana, alteza real a Grã-duquesa do Luxemburgo, e a majestade rainha dos Países Baixos tratando de dados pessoais, em seu artigo 16º[58], itens "1" e "2", mas no âmbito das autoridades públicas.

Em 28/01/1981, a Convenção do Conselho da Europa (Convenção de Strasbourg) resolveu proteger o tratamento dos dados pessoais automatizados[59], com a finalidade de proteger e aplicar

---

[57] Tratado sobre o Funcionamento da União Europeia. Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF. Acesso 21/06/2021.

[58] **Art. 16**. *(ex-artigo 286.o TCE) 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. O Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário, estabelecem as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes.*

[59] Universidade de Coimbra. Informação Administrativa e Proteção de Dados. Disponível em: <https://www.uc.pt/protecao-de-dados/protecao_dados_pessoais/da_privacidade_a_protecao_de_dados>. Acesso 21/06/2021.

medidas punitivas contra o preconceito, a *cyber* criminalidade, o racismo, a xenofobia, a falsificação de documentos administrativos e o seu tráfico, a falsificação de meios de pagamento, e nestes dois últimos pode-se subentender certa preocupação ali sobre utilizar falsamente os dados pessoais de outros indivíduos.

Então, em 24 de Outubro de 1995, o Parlamento Europeu e o seu Conselho[60] resolveram legislar especificadamente sobre a proteção dos indivíduos, e já muda o texto e as nomenclaturas das palavras, trazendo o tratamento de dados pessoais na comunidade europeia por meio da diretiva 95/46/CE do Parlamento Europeu e do Conselho datada de 24/10/1995 sobre a proteção das pessoas, no que diz respeito ao tratamento de dados pessoais e a livre circulação desses dados, tendo o Parlamento Europeu, o Conselho da União Europeia se reunido para preservar os dados pessoais em razão das trocas econômicas feitas entre os povos europeus e, desta forma, o objetivo era fomentar as relações entre os estados que pertencem a essa comunidade, assegurando o seu processo econômico e social, sem quaisquer barreiras, sempre com o olhar para a paz e para a liberdade na promoção da democracia, pautada na Convenção Europeia dos Direitos Humanos.

Em tão logo de suas considerações de número “4”[61], a diretiva 95/46, resolveu proteger o tratamento dos dados, reconhecendo que o seu uso é frequente na comunidade europeia e que o avanço da tecnologia da informação facilita a transferência de dados. Em ato

---

[60] Diretiva 95/46/CE Parlamento Europeu e do Conselho. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046. Acesso 21/06/2021.

[61] [...] (4) *Considerando que o recurso ao tratamento de dados pessoais nos diversos domínios das actividades económicas e sociais é cada vez mais frequente na Comunidade; que o progresso registado nas tecnologias da informação facilita consideravelmente o tratamento e a troca dos referidos dados*. [...] [correção de ortografia nossa]

contínuo, em sua consideração de número “7”[62], a comunidade europeia reconhece que há diferenças no tratamento de dados pessoais entre os Estados-membros e que essa diferença poderia ser um obstáculo para as atividades econômicas da comunidade, inclusive, atrapalhar na concorrência com as diferentes legislações entre os países que compõem a União Europeia.

Percebe-se que, aqui nesta diretiva, que o legislador já trata os dados atinentes à saúde como dados pessoais sensíveis e sua respectiva e poderosa importância no domínio dos tratamentos e na preocupação com a sua constante proteção.

Esta diretiva traz um importante traço sobre o tratamento de dados de um país ao outro, da qual ela proíbe a transferência de dados de uma empresa para a outra em que determinado país que a recebe e não ofereça a segurança necessária, neste caso, essa transferência fica terminantemente proibida, obedecendo normas específicas da Decisão 87/373/CEE do Conselho[63].

Essa diretiva conceitua dados pessoais como qualquer informação relativa a uma pessoa singular identificada ou identificável (pessoa em causa); é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência

---

[62] [...] (*7) Considerando que as diferenças entre os Estados-membros quanto ao nível de protecção dos direitos e liberdades das pessoas, nomeadamente do direito à vida privada, no domónio* do tratamento de dados pessoais, podem impedir a transmissão desses dados do território de um Estado-membro para o de outro Estado-membro; que estas diferenças podem, por conseguinte, constituir um obstáculo ao exercício de uma série de actividades económicas à escala comunitária, falsear a concorrência e entravar o exercício pelas administrações das funções que lhes incumbem nos termos do direito comunitário; que esta diferença de níveis de protecção resulta da disparidade das disposições legislativas, regulamentares e administrativas nacionais.* [...] *[Texto original]

[63] *Publications Office of the EU. 87/373/CEE.* Decisão do Conselho de 13 de Julho de 1987. Disponível em: https://op.europa.eu/en/publication-detail/-/publication/f742e9e6-3ef9-4ec1-83ec-8dc1a5d2dd09/language-pt. Acesso 21/06/2021.

ao número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social.

Percebe-se que, também se traz já a palavra “consentimento” utilizando-se o termo de consentimento da pessoa em causa, qualquer manifestação da vontade livre e específica é informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objeto de tratamento.

O Regulamento CE n. 1338/2008[64] do Parlamento Europeu e do respectivo Conselho traz um trecho interessante sobre igrejas, cuja escolha pela crença e religião foi e ainda continua sendo alvo de ataques preconceituosos. As instituições religiosas são consideradas para fins de estudos e aplicações do Poder Público de interesse da coletividade, pois o direito está elencado na Constituição e no Direito Internacional Público.

E vale destacar sobre a Inteligência artificial neste cenário de proteção de dados, pois ela é capaz de determinar as decisões dos titulares com base na análise das preferências, comportamentos e atitudes, por isso, empresas que controlam o comportamento de pessoas deverão informar como elas são seguidas na internet e o limite do potencial alcançado deste perfil traçado, principalmente no campo internacional, onde ela é bem explorada, por isso, este trabalho tem o condão de fazer alertas também sobre o seu uso, e como manter precauções responsáveis para as empresas não deixarem de usá-la.

Quando se fala sobre proteção de dados pessoais no Brasil, antes de adentrarmos no cenário específico, efetivamente, pela linha do tempo que vem demonstrando neste capítulo, discorrer-se-á por todas as legislações brasileiras quais já haviam discretamente abordado o assunto, com outras denominações, mas que, por exemplo, empresas multinacionais quais já possuíam por cultura o padrão “GDPR” (*General*

[64] Regulamento (CE) n. o 1338/2008 do Parlamento Europeu e do Conselho de 16 de Dezembro de 2008. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32008R1338. Acesso 21/06/2021.

*Data Protection Regulation*)[65] deveriam ter, ao menos, iniciado alguma adequação em proteção de dados pessoais.

Após o escândalo que ocorreu no cenário internacional trazido no primeiro capítulo sobre a empresa Cambridge Analytica, que apesar da Europa já ter estabelecido a Diretiva 95/46. Com este acontecimento, e em razão das graves acusações que foram expostas e que o *facebook* não conseguiu se explicar muito bem, a diretiva foi então revogada pelo Regulamento 679, de 27 de abril de 2016, conhecido como Regulamento Geral sobre Proteção de Dados ou, em inglês, como General Data Protection Regulation da União Europeia - 2016/679 (GDPR)[66].

Este regulamento ainda continua a explicitar sobre a proteção a vida privada e familiar, trazida anteriormente pelas demais legislações, em sua consideração "4"[67], lastros de defesa da religião e crenças, ainda continuando com o espírito da diretiva de eliminar barreira entre os países e a prevalência de equivalência de proteção de dados pessoais perante os Estados que compõe a União Europeia (consideração "9").

É uma Lei geral que se aplica no setor público e no setor privado, pelo modelo europeu com a intenção de dar maior uniformidade par a proteção de dados pessoais na Europa.

Conhecido pela sigla RGPD, o regulamento deu novas diretivas em relação ao regulamento de 95/46/CE, apesar de manter acesa a validade dos princípios e objetivos, deu outras orientações sobre a

---

[65] Trabalho de campo realizado na Advocacia Baccari nas consultorias a multinacionais e palestras que realizei desde junho de 2019.

[66] Regulamento (UE) 2016/ 679 do Parlamento Europeu e do Conselho. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679. Acesso 21/06/2021.

[67] *(4) O tratamento dos dados pessoais deverá ser concebido para servir as pessoas. O direito à proteção de dados pessoais não é absoluto; deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade. O presente regulamento respeita todos os direitos fundamentais e observa as liberdade* e os princípios reconhecidos na Carta, consagrados nos Tratados, nomeadamente o respeito pela vida privada e familiar, pelo domicílio e pelas comunicações, a proteção dos dados pessoais, a liberdade de pensamento, de consciência e de religião, a liberdade de expressão e de informação, a liberdade de empresa, o direito à ação e a um tribunal imparcial, e a diversidade cultural, religiosa e linguística.**[Erro do texto original]

proteção e tratamento de dados de pessoas vivas no âmbito eletrônico, por causa do aumento significativo dos fluxos transfronteiriços de dados pessoais que transformaram a economia e a vida social com a nova tecnologia digital.

Dessa maneira, a União Europeia, por meio deste regulamento, previu a necessidade rígida de proteger os dados dos titulares com o objetivo de gerar segurança jurídica e segurança prática nesse mercado que passou a fomentar o desenvolvimento da economia digital de pequenas, médias e grandes empresas, compelindo obrigações, responsabilidades e até sanções.

O RGPD não apenas atualizou a regulamentação, mas pretendeu garantir a eficácia, reforçando e especificando os direitos dos titulares dos dados, impondo obrigações aos responsáveis pelo tratamento de dados, definindo os direitos dos titulares e poderes dos controladores, descrevendo regras e sanções no caso de haver infrações ao estabelecido.

O interessante é a imposição que o GDPR traz para as empresas tratarem os dados por meio automatizado e manual às pessoas identificáveis e identificadas[68], mesmo que, para isso, seja necessária a utilização de ferramentas tecnológicas avançadas versus o tempo que será dispendido para tanto. O que se pode fazer por analogia com as empresas de investimentos em *criptomoedas* nas quais os que possuem os seus investidores anônimos (em números), mas que podem ser identificáveis por meio de uma wallet, permaneçam corretamente inscritos.

Apesar do regulamento objetivar o uso da tecnologia, ele não traz a obrigatoriedade de algum tipo de sistema tecnológico, como

---

[68] *(67) Para restringir o tratamento de dados pessoais pode recorrer-se a métodos como a transferência temporária de determinados dados para outro sistema de tratamento, a indisponibilização do acesso a determinados dados pessoais por parte dos utilizadores, ou a retirada temporária de um sítio web dos dados aí publicados. Nos ficheiros automatizados, as restrições ao tratamento deverão, em princípio, ser impostas por meios técnicos de modo a que os dados pessoais não sejam sujeitos a outras operações de tratamento e não possam ser alterados. Deverá indicar-se de forma bem clara no sistema que o tratamento dos dados pessoais se encontra sujeito a restrições.*

também não determina qual técnica deve ser aplicada. Não obstante, a identificação do titular pode ser por IP, *cookie* ou etiquetas de identificação por radiofrequência, e esses informes devem ser trazidos à transparência do indivíduo.

O GDPR também traz o Termo de Consentimento[69] do titular dos dados que deverá ser claro, específico, conciso, incontroverso ao fim de que se destina, e assinado de maneira livre, que poderá ser por escrito, por meio eletrônico, ou até por uma declaração oral, sendo claro que a omissão não caracteriza por este regulamento uma permissão de seu consentimento.

Impõe-se trazer informação sobre o campo da saúde, cujo dado pessoal é tratado como sensível: os dados pessoais genéticos deverão ser resultados de amostra biológica de cromossomos, ácido desoxirribonucleico, ou ácido ribonucleico[70].

Assim, no assunto da saúde completa, os dados da pessoa serão considerados o seu passado, presente e futuro sobre a saúde física e/ou mental por uma doença, deficiência, risco de doença, histórico clínico, tratamento clínico ou estado fisiológico ou biomédico.

---

[69] (*32) O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrónico, ou uma declaração oral. O consentimento pode ser dado validando uma opção ao visitar um sítio web na Internet, selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais. O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento. O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins. Se o consentimento tiver de ser dado no seguimento de um pedido apresentado por via eletrónica, esse pedido tem de ser claro e conciso e não pode perturbar desnecessariamente a utilização do serviço para o qual é fornecido.*

[70] Consideração de n. 34 do GDPR.

O regulamento já define onde deverá ficar estabelecido o responsável pelo tratamento, é o local onde se encontra a administração.

Para se garantir a segurança e até a confidencialidade dos dados tratados, a regulamentação prevê que o controlador aponte um prazo a ser estabelecido para o tratamento daquele dado, e qual o período de revisão a qual ele está sujeito, ou seja, quando ele será apagado?

Quando há um conglomerado de empresas tidas como grupo empresarial ou instituição associada à empresa que tratam dos dados dos titulares, deverão haver princípios regentes desta transmissão de informações, especialmente sobre a segurança que lhes será imputada, o que pode-se citar como exemplo, é uma empresa de segurança da informação e da rede que compromete com o seu cliente a resistir a um determinado nível de segurança a eventos acidentais e/ou ações maliciosas ou ilícitas que comprometam a disponibilidade, autenticidade, integridade, a confidencialidade dos dados pessoais conservados ou transmitidos e da própria rede e sistemas que a compõem.

As informações de interesse público não atingem o sigilo que determina, assim como as informações que forem consideradas vitais para a vida do titular e que são monitoradas durante epidemias, pandemias e catástrofes em emergência humanitária.

Outro direito que também deverá ficar disponível ao Poder Público por se tratar de proteção social são informações para o fim de segurança e gestão dos serviços de saúde para a sua monitorização, alerta, prevenção e controle de doenças transmissíveis e graves.

Já no Brasil, senão, vejamos, a Constituição Federal – 1988, em seu artigo 05º, X[71] menciona sobre a privacidade, um direito

[71] **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:*

fundamental, qual sua previsão vem desde 1988, pretende-se frisar o ano, porque não é fundamento para as empresas tal desconhecimento legal, que somente aguardaram a vigência em sua maior parte dos artigos da Lei Geral de Proteção de Dados Pessoais, e a criação da Autoridade Nacional de Proteção de Dados para então, tomar frente de algo.

O filósofo Márcio Pugliesi foi o primeiro diretor do Departamento Nacional de Proteção e Defesa do Consumidor da Secretaria de Direito Econômico e do Ministério da Justiça. Ele foi responsável por conduzir a aprovação do Código de Defesa do Consumidor no Congresso Nacional[72].

O Código de Defesa do Consumidor – 1990, em seu artigo 43[73], trata sobre o consentimento, que ele não é único meio para se legitimar

---

*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.* [...]

[72] LINKEDIN. 2020 Disponível em: <https://br.linkedin.com/in/marcio-pugliesi-96924322>, com acesso em 23/09/2020.

[73] *Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.*

*§ 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.*

*§ 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.*

*§ 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.*

*§ 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.*

*§ 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer*

um ato de tratamento de dados, isso significa interpretar que a vontade do titular legitima o seu consentimento.

Apesar de ser de cunho financeiro, porém, com grande banco de dados, a instituição financeira ganhou uma disposição sobre o sigilo de suas operações com a Lei Complementar 105 – 2001[74].

Em 2002, o Código Civil, trouxe o texto do artigo 21[75] e se dedicou a prescrever o direito à vida privada, exaltando o direito de inviolabilidade, inclusive, com medidas que se tornem necessárias para a sua consecução e cumprimento, com a finalidade de impedir ou fazer parar essa violação, com a proteção do Estado, e neste trecho da Lei, percebe que a filosofia está entrelaçada com o direito, uma vez que a proteção do indivíduo se dá incialmente em proteção ao Estado, teoria do Diálogo das Fontes, idealizada por Erik Jayme e trazida ao Brasil por Cláudia Lima Marques[76].

A Lei de Acesso à Informação − Lei 12.527/2011[77], foi conquista do cidadão antenado com o envolvimento eletrônico trouxe uma

---

*informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.*

*§ 6o Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor. (Incluído pela Lei nº 13.146, de 2015) (Vigência)*

[74] Lei Complementar nº 105, de 10 de Janeiro de 2001. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/LCP/Lcp105.htm>. Acesso 21/06/2021.

[75] **Art. 21**. *A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma. (Vide ADIN 4815)*

[76] PUC. 2020. Aula de proteção de dados pessoais no curso de LGPD na instituição "Meu Curso" em janeiro de 2020.

[77] Lei nº 12.527, de 18 de Novembro de 2011. **Disponível em: <**http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm>. Acesso 21/06/2021.

visibilidade para que pudesse ter mais acesso ao armazenamento de seus dados, e as primeiras empresas que tiveram impacto direto com esse dever de garantir o direito fundamental ao acesso das informações de dados pessoais foram os órgãos públicos (Poderes Executivo, Legislativo, e Judiciário; e Ministério Público; todas autarquias, fundações, sociedade de economia mista e empresas públicas controladas pela União, Distrito Federal, Municípios e Estados; empresas privadas sem fins lucrativos que recebem recursos públicos).

É necessário notar que a partir desta Lei, o legislador usou o serviço da tecnologia da informação a favor do Governo, que foi citado como diretriz para se utilizar dos meios de comunicação a obtenção do cidadão ao acesso aos seus dados pessoais.

Esta Lei prevê a obrigatoriedade do Poder Público em controlar todas as informações pessoais de maneira transparente, devendo propiciar acesso amplo ao titular e cuidado com a divulgação, pois ele deve protegê-la, garantindo a sua disponibilidade no sistema de forma autêntica e íntegra, além de dever ter o zelo para julgar se a informação é sigilosa e merece restrição de acesso.

O legislador já predeterminou uma norma da qual o governo deveria ter em seu planejamento para atendimento desta Lei.

Assim, é possível traçar um histórico no Brasil desde a promulgação desta Lei, para ser diretriz de uma execução perfeita para o assunto que queremos chegar: como adequar uma empresa às normas da LGPD?

Mas antes, volta-se à análise da cartilha (regulamento) que deve ter cada ente ou empresa pública (equiparada) que armazene em registros ou documentos, produzidos ou acumulados por seus órgãos ou entidades, recolhidos ou não a arquivos públicos informação produzida ou custodiada por pessoa física ou entidade privada, decorrente de qualquer vínculo com seus órgãos ou entidades, mesmo que esse vínculo já tenha cessado, com exceção de projetos de pesquisa e desenvolvimento científicos ou tecnológicos cujo sigilo seja imprescindível à segurança da sociedade e do Estado.

A informação tratada deve respeitar a transparência, à intimidade, a vida privada, a honra, a liberdade, as garantias individuais e a imagem do titular, da seguinte maneira:

I. Deve ser esclarecido como o titular tem acesso a essa informação, indicando a competência de cada pessoal e a estrutura organizacional, indicar um local (de fácil acesso) onde ela está armazenada com número de telefone, endereço físico e eletrônico e horário de atendimento ao público, de modo a garantir que esse acesso atenda também as pessoas com deficiência.

II. Deve ser assegurado ao titular que a informação seja primária, íntegra, autêntica e atualizada.

III. Deve informar ao titular como funciona essa atividade de registro e armazenamento de dados, divulgando, inclusive a sua política, organização e serviços que dispõe para que tudo aconteça em conformidade com a Lei.

IV. Essa informação ao titular deve ser realizada em relatório de texto e planilha, gravada em diversos formatos eletrônicos.

V. O acesso à essas informações, deve ser automatizado por sistemas externos em formatos abertos, estruturados e legíveis por máquina.

VI. Deve conter, inclusivamente, informações de domínio público de qualquer cidadão brasileiro nato ou naturalizado deva saber sobre a administração do patrimônio público, utilização de recursos públicos, licitação, contratos administrativos; a implementação, acompanhamento e resultados dos programas, projetos e ações dos órgãos e entidades públicas, bem como metas e indicadores propostos de resultado de inspeções, auditorias, prestações e tomadas de contas realizadas pelos órgãos de controle interno e externo, incluindo prestações de contas relativas a exercícios anteriores.

VII. Informar ao titular se a informação de seus dados foi extraviada, podendo abrir processo interno de sindicância para

apurar o desaparecimento da respectiva documentação e prestar esclarecimentos ao titular.

VIII. Indicar o responsável pela guarda da informação extraviada, que terá o prazo de 10 (dez) dias para justificar o fato e indicar testemunhas que comprovem sua alegação.

IX. Deve assegurar que as informações restritas consideradas sigilosas como ultrassecretas, secretas ou reservadas sejam protegidas, inclusive dispondo procedimentos e medidas a serem adotados para o tratamento de informação sigilosa, de modo a protegê-la contra perda, alteração indevida, acesso, transmissão e divulgação não autorizados.

X. A informação sigilosa somente poderá ser divulgada com consentimento expresso (autorização) do titular e/ou por meio de previsão legal.

XI. Deve garantir o treinamento do pessoal subordinado às informações sigilosas para que conheçam das normas.

XII. Deve ter registrada as despesas, transferências, repasses a qualquer empresa ligada a administração pública direta e/ou indireta de contratos ou licitações.

XIII. Deve indicar dados gerais de programas, ações, projetos e obras ao titular do direito.

XIV. Deve ter em sua cartilha um conjunto de perguntas e respostas mais frequentes.

Perceba que o legislador já havia legalizado qual meio de comunicação seria escolhido para publicização e armazenamento dessas informações que as empresas públicas e equiparadas devem fornecer ao titular de direito, cujo local obrigatório se daria pela internet (rede de computadores) e por diversos formatos eletrônicos.

O legislador garantiu a efetividade da Lei quando previu a criação de atendimento específico para que a participação da sociedade fosse real quanto aos seus direitos sobre as informações e armazenamentos de seus dados.

O que deverá ocorrer também, com o vigor da LGPD, que por enquanto, só tem a previsão da fiscalização, que será explicado adiante.

Esse serviço específico deve atender:

I. Profissional habilitado para orientar ao titular sobre todos os seus direitos reservados nesta Lei.

II. Realizar protocolos de pedidos referente a acesso às informações.

III. Informar sobre o andamento do processo administrativo.

IV. Ter um setor de conciliação para atender demandas que poderão se tornar judicializadas.

V. Criar programas de incentivo à população sobre a ciência desta Lei.

A restrição sobre o acesso à informação ultrassecreta, secreta, ou reservada, já que essas empresas tratadas aqui neste capítulo são de natureza pública ou equiparadas às públicas, é sobre qualquer informação que coloque em risco a defesa e a soberania nacionais ou integridade do território nacional; prejudicar ou colocar em risco as forças armadas, projetos de pesquisa e desenvolvimento científico ou tecnológico, sistemas, bens, instalações ou áreas de interesse estratégico nacional; as tratativas internacionais, que tenham sido consideradas sigilosas por outros países; oferecer alto risco sobre a economia monetária e financeira do Brasil, colocar em risco a vida, saúde ou segurança da população, a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares; comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações.

As práticas dessas empresas que levam a uma infração se resumem a:

1. Se recusar, retardar, ou a fornecer informação de forma intencionalmente incorreta, incompleta ou imprecisa.

2. Utilizar indevidamente, subtrair, destruir, inutilizar, desfigurar, alterar, ocultar ou destruir, total ou parcialmente informação.

3. Agir com dolo ou má-fé no acesso aos dados e informações.

4. Divulgar, acessar ou permitir acesso indevido à informação sigilosa ou informação pessoal.

5. Impor sigilo à informação para obter proveito pessoal ou de terceiros.

6. Ocultar informação sigilosa a autoridade para beneficiar a si ou a outrem.

Além do infrator cometer crime de improbidade administrativa, conforme o disposto nas Leis n. 1.079/ 1950, e 8.429/1992, terá as seguintes penalidades: advertência; multa; rescisão do vínculo com o Poder Público; suspensão temporária para participar de licitação e impedimento de contratar com a administração pública por prazo de até 02 (dois) anos; declaração de inidoneidade para licitar ou contratar com a administração pública, até a efetiva reabilitação.

Nesta Lei, verifica-se que o legislador previu a criação de dois órgãos apartados para assegurar o disposto legislativo, a Comissão Mista de Reavaliação de Informações que cuida sobre o tratamento e a classificação de informações sigilosas no âmbito da Administração Pública Federal e o Núcleo de Segurança e Credenciamento (NSC) qual sua função é propor justamente a regulamentação do credenciamento de pessoas físicas, empresas, órgãos e entidades que tratam das informações sigilosas, bem como, promover e garantir essa segurança da informação proveniente do Brasil ou do estrangeiro.

O Poder Executivo Federal deverá designar um órgão da administração pública federal, que será a responsável por promover uma campanha de conscientização do direito fundamental ao acesso à informação da população, e essa campanha deverá abranger o território nacional.

Após anos sem penalização para qualquer tipo de pena de crimes cometidos em meio virtual, a Lei Carolina Dieckmann - Lei 12.737/

2011[78] ficou conhecida porque a atriz cujo nome se deu a Lei teve o seu conteúdo de arquivo privado acessado quando em sua rotina enviou o seu *notebook* para um reparo eletrônico, que a partir de então, tiveram vazadas imagens e conversas de cunho íntimo e que lhe trouxeram devastadores dissabores e atentados criminosos contra a sua honra. Acontece que, no Código Penal de 1940 não havia a previsão para crime eletrônico desta natureza, e então, veio a Lei 12.737 de 2012 com a previsão da tipificação penal para os delitos cometidos no âmbito da internet, alterando assim o Decreto-Lei de número 2.848 de 07 de dezembro de 1940[79].

Fica bem claro o que a sociedade não acompanhou a evolução dos acontecimentos civis, já que o legislador demorou 72 anos para tipificar um crime ocorrido no âmbito eletrônico, cuja navegação no Brasil já era prevista desde 1992 pelo doutrinador e professor João Antônio Zuffo[80].

É possível notar pela escrita da Lei que ela trouxe o consentimento expresso em seu texto, pois por razões óbvias, na seção do Código Penal que trata sobre os crimes contra inviolabilidade dos segredos, que é um título de origem sigilosa. Desta forma, não poderia a informação ser tratada de outra maneira, a não ser de acesso restrito a quem dela o titular da informação não lhe der autorização para o acesso.

---

[78] Lei nº 12.737, de 30 de Novembro de 2012. **Disponível em** http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm.>. Acesso 21/06/2021.

[79] Decreto-lei nº 2.848, de 7 de Dezembro de 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848.htm>. Acesso 21/06/2021.

[80] ZUFFO, João Antonio. **A Infoera: O Imenso Desafio do Futuro.** São Paulo: Editora Saber Ltda., 1997, p. 14.

O artigo inserido sobre a invasão de dispositivo informático está atrelado a violação de segredo profissional porque neste caso, a atriz ao levar o seu *notebook* para o único local que teria acesso às informações, o profissional responsável pelo reparo se utilizou de sua profissão para acessar local onde estavam armazenadas as fotos íntimas da atriz, por essa razão, tornou-se crime a invasão ou conexão de dispositivo informático ligados ou não há uma rede de computadores sem autorização expressa para obter, adulterar ou destruir dados/informações obtendo vantagem ilícita.

O legislador ainda previu a tipificação de outros crimes realizados por meio de acesso informático, telefone, telemático, telegráfico, mas não serão temas de abordagem nesta ocasião.

O sigilo das informações e a forma com que elas e os dados pessoais podem ser acessados também faz parte de uma conquista para trazer a este trabalho, pois a Lei de Cadastro Positivo – 12.414/ 2011[81] também trata daqueles dados excessivos que são anotados no cadastro da pessoa, e esse texto vai de encontro com uma das formas de se trabalhar os dados pessoais erradamente, trazidos pela LGPD. Assim, faz necessário o entendimento desta Lei para compreensão total de proteção e do mecanismo que é proposto aqui.

Em 23 de abril de 2014, o Marco Civil da Internet – Lei 12.965/2014, em meios aos desafios da infoera, surgiu para ir além de dizer qual o direito e dever do cidadão que faz uso da internet, de nortear o acesso a princípios e garantias, mas de alcançar o objetivo de disseminar as novas tecnologias e uso de acesso a todos, preferencialmente pelos meios eletrônicos, as informações, principalmente de assunto público e assim ter alcance mais rápido e racionalizado a toda população.

O fundamento do marco civil da internet é o respeito a liberdade de expressão da pessoa aos meios digitais.

---

[81] Lei nº 12.414, de 9 de Junho de 2011. **Disponível em:** https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>. Acesso 21/06/2021.

O uso da rede social pressupõe alguns princípios básicos como a liberdade de expressão, comunicação e a manifestação de pensamento com a finalidade de que cada um tenha protegida a sua privacidade, e os seus dados pessoais.

Além da preocupação com a privacidade do usuário da internet, o legislador trouxe nesta lei, a garantia de medidas técnicas utilizadas internacionalmente, para o fim de segurança e funcionalidade da rede.

Mesmo diante de um cenário cheio de regras, e impulsionado pelas boas práticas de convivência com os demais usuários, outro princípio que norteia essa convivência saudável são as sanções e penas trazidas pela responsabilização de cada usuário ou site de acesso que vão de advertência, multa de até 10% do faturamento do último exercício do grupo econômico no Brasil, suspensão temporária das atividades, proibição de coleta, armazenamento, guarda ou tratamento de dados, ou de comunicações, danos materiais e morais.

É certo que, de acordo com essa passagem histórica legislativa traçada, não poderia ser diferente o Marco Civil da Internet ter mantido as garantias da inviolabilidade, da intimidade, da vida privada, a honra, a imagem e os sigilos das informações trazidas pelos seus titulares, onde quer que elas estejam armazenadas, mas é importante fazer um conexão com a LGPD que será trazida à frente, pois além de proteger as informações, ela protege o tratamento das informações, os registros das conexões, e o acesso que o usuário fez de aplicações na internet para que não seja repassado à terceiros.

As únicas exceções de divulgação dessas informações só podem ocorrer na hipótese de autorização judicial ou de consentimento livre e expresso do titular do dado.

Ao fornecedor da internet, foi lhe dado o dever desde o início da contratação, que deverá conter informações claras e completas sobre o regime de políticas internas que protejam o registro da conexão e do acesso à internet, e do afeto a instabilidades no sistema, mantendo a conexão, a manutenção e qualidade na prestação de serviços desta natureza, salvo de houver falta de pagamento do usuário.

Os sigilos das informações continuaram sendo tratados pelo legislador de forma cuidadosa, já que para tratar do armazenamento pelo período que dispõe a Lei (um ano), é necessário um setor próprio de segurança que não poderá ser contratado por terceiros, isso significa, que a própria empresa quem deverá ser responsável por esse ambiente controlado.

Em 12 de novembro de 2014, o STJ julgou o recurso especial REsp 1.457.199 [(RS 2014/0126130-2) ANEXO I] da qual tratou muito bem sobre questões envolvendo a tríade tratada pelo filósofo Márcio Pugliesi, inclusive, tratando explicitamente sobre os temas de privacidade, intimidade e publicidade, modelo alemão, que foi estudado pelo Filósofo brasileiro. Veja, o ministro Relator Tarso, explica a ideia de publicidade o que é a área de atuação pública de cada pessoa, exposta ao interesse público em geral, e que, consequentemente, apresenta a livre atuação pelos meios de comunicação em geral. A privacidade é uma esfera intermediária, cuja proteção é inversamente proporcional ao estatuto social da pessoa assim quanto mais pública a pessoa menor grau de proteção. A intimidade é o último e inviolável reduto da liberdade pessoal, que não pode ser devassada por mais pública que seja a pessoa[82]. Que os ministros Maria Isabel Gallotti, Antônio Carlos Ferreira, Ricardo Villas Bôas Cueva, Marco Aurélio Bellize, João Otávio de Noronha e Raul Araújo votaram com o ministro relator Paulo de Tarso San Severino, que foi muito feliz em toda a sua fundamentação jurídica da qual se vê muito do que este trabalho trouxe.

O suprarreferido acórdão se empenhou em analisar os artigos vigentes até aquele momento 12/11/2014, em que não havia a existência da Lei Geral de Proteção de Dados, isso significa entender que o instituto jurídico demarcou processos de *compliance* na prestação de serviço de

[82] SUPERIOR TRIBUNAL DE JUSTIÇA, 2020. Recurso Especial n. 1.457.199 - RS. Disponível em: <https://bdjur.stj.jus.br/jspui/bitstream/2011/114173/REsp1457199.pdf>. Acesso 23/09/2020.

inteligência artificial que analisa dados e classifica-os gerando uma nota de crédito ao consumidor (titular dos dados). São eles: conceito de “credit scoring”; avaliação do risco de crédito nos contratos em geral; regulamentação dos arquivos de consumo pelo Código de Defesa do Consumidor; a Lei do Cadastro Positivo (Lei 12.414/2011); licitude do sistema “credit scoring”; limites da privacidade e transparência e do dano moral.

Esses pontos norteados pelo acórdão contribuíram para o desenvolvimento deste trabalho de maneira significativa quando da descrição da linha de tempo das legislações brasileiras e reflexões sobre o cenário de transparência que os prestadores de serviços já deveriam ter com os titulares de dados pessoais, pois puderam trazer sinais de obrigatoriedade com o Princípio nuclear da LGPD que é justamente o Princípio da Transparência.

A Súmula 550 do Supremo Tribunal .de Justiça[83] publicada em 19/ de outubro de 2015, no primeiro momento a inclusão automática e no segundo momento *opt-out*, inclusive que o indivíduo pode pedir esclarecimentos das informações que lhe foram valoradas para o cálculo do crédito, isso significa mais um salto alcançado na sociedade brasileira, garantindo que o dado pessoal corresponde a pessoa, e que o conjunto desses dados dão informações relativas à pessoa, construindo valores que lhe são pertinentes a si próprio e exclusivamente.

E após essa linha do tempo trazida para contribuir com as reflexões e se formar um entendimento do quão importante é a proteção de dados pessoais, chegou a vez da queridinha LGPD, nascida em

[83] **Súmula 550 do STJ**: *A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo*. [grifo nosso]

14/08/2018 - Lei Geral de Proteção de Dados Pessoais – Lei 13.709/2018[84].

Com o avanço da tecnologia a serviço da informação cada vez mais rápida e ao alcance da sociedade, que vive conectada a internet e está por dentro dos seus direitos, o Estado se viu obrigado a garantir ao cidadão o acesso à informação de forma transparente, clara e em linguagem de fácil compreensão.

A LGPD, apesar do seu texto trazer informações genéricas, no Brasil, é a Lei mais específica que trata sobre o tema proteção de dados pessoais, reunindo palavras encontradas em textos de Lei internacional, separadas anteriormente, e neste texto, o legislador procurou unificar também os sentidos, por isso, a sua leitura deve ser antecedida de toda a legislação trazida, pois ela é plano de fundo, principalmente do GDPR, regulamento mais atualizado da União Europeia que trata do assunto de forma completa.

A Lei Geral Proteção de Dados Pessoais tem como objetivo a proteção de dados pessoais da pessoa física, como direito de privacidade, liberdade e o livre desenvolvimento da personalidade da pessoa natural, isso significa entender que as empresas públicas e privadas e inclusive, autônomos que prestem serviço sob a troca de moeda financeira, terão que seguir as diretrizes da LGPD.

O essencial da LGPD é o respeito à privacidade, a preservação da honra, da imagem, e da intimidade, dos direitos humanos, da dignidade, da personalidade, de modo que as pessoas possam exercer a cidadania em meio a todo desenvolvimento tecnológico da nova sociedade de dados com proteção a liberdade de expressão, de informação, de comunicação, e de opinião do consumidor (indivíduo).

---

[84] Lei Geral de Proteção de Dados Pessoais – Lei 13.709/2018. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm>. Acesso 22/06/2021.

O cerne geral da LGPD é o tratamento de dados pessoais[85] coletados e tratados em território brasileiro com finalidade comercial e econômica.

Quando se faz uma leitura desta Lei é necessário distinguir as palavras de privacidade, intimidade, publicidade, que brilhantemente foram trazidas pela Relator Ministro Excelentíssimo Senhor Tarso, conforme supraexposto, da qual vem sendo constantemente firmados os entendimentos de que as informações e dados pessoais são da pessoa, por mais que, os dados pessoais tenham sido cadastrados por empresas; veja o cadastro é da empresa, contudo, as informações pessoais e dados pessoais cadastrados são da pessoa, exclusivamente.

Por isso, a relevância da construção histórica e das legislações internacionais mais respeitadas sobre este tema, para que se mostre as empresas como o indivíduo foi desrespeitado ao longo do tempo, e que mesmo após conquistados esses direitos sendo elencados como fundamentais e do capítulo de direitos humanos, continuaram sendo escrachados pelas empresas, sem muitos cuidados, e sem um *compliance* adequado ou sistematicamente organizado que garanta a segurança do seu armazenamento e o seu tratamento de modo geral, por mais que a Europa tenha desde 1948 definições sobre o tema.

A Lei Geral de Proteção de Dados Pessoais também tratou de mencionar sobre o dado pessoal sensível, aquele dado pessoal sobre origem racial ou étnica, convicção religiosa opinião política, filiação a sindicato ou 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 (Artigo 5º, II da Lei 13.709/2018[86]),

---

[85] Dado pessoal é informação relacionada à pessoa natural identificada ou identificável, de acordo com o artigo 05º, I da Lei 13709 de 2018.

[86] **Art. 5º**. *Para os fins desta Lei, considera-se: [...]*

*II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso,*

porque trouxe no DNA da GDPR que seria de suma importância o rigoroso tratamento dado aos dados pessoais, sobretudo aos dados pessoais sensíveis porque deles, como foi visto decorreu no passado o extremo preconceito e discriminação do manuseio errado dessas informações, podem causar sérias gravidades invariáveis em que o dano social pode ser físico, material ou imaterial com prejuízos à reputação de cunho até que irreversíveis ao indivíduo. Em análise com o trazido no texto da GDPR, pode-se entender a extensão da atualização do que seria dado pessoal sensível, veja que em sua consideração "75"[87] (...Origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical, bem como dados genéticos ou dados

*filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.* [...]

[87] *(75) O risco para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, poderá resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, em especial quando o tratamento possa dar origem à discriminação, à usurpação ou roubo da identidade, a perdas financeiras, prejuízos para a reputação, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, à inversão não autorizada da pseudonimização, ou a quaisquer outros prejuízos importantes de natureza económica ou social; quando os titulares dos dados possam ficar privados dos seus direitos e liberdades ou impedidos do exercício do controlo sobre os respetivos dados pessoais; quando forem tratados dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical, bem como dados genéticos ou dados relativos à saúde ou à vida sexual ou a condenações penais e infrações ou medidas de segurança conexas; quando forem avaliados aspetos de natureza pessoal, em particular análises ou previsões de aspetos que digam respeito ao desempenho no trabalho, à situação económica, à saúde, às preferências ou interesses pessoais, à fiabilidade ou comportamento e à localização ou às deslocações das pessoas, a fim de definir ou fazer uso de perfis; quando forem tratados dados relativos a pessoas singulares vulneráveis, em particular crianças; ou quando o tratamento incidir sobre uma grande quantidade de dados pessoais e afetar um grande número de titulares de dados.*

relativos à saúde ou a vida sexual ou a condenações penais em infrações ou medidas de segurança conexas...).

Ao que tudo indica, a definição de um perfil traçado com esses dados sensíveis torna a pessoa mais vulnerável, porque daí a empresa pode fazer análise sobre visões que dizem respeito a qualquer ato da vida civil que o indivíduo possa fazer ou realizar, inclusive, sobre as suas preferências e os seus interesses pessoais. Imagine que este perfil seja traçado por um sistema de inteligência artificial nos quais o controlador dessa informação não tenha um mínimo de aplicabilidade ou regulamento de normas de segurança em sua empresa para o manuseio e tratamento desses dados, sendo um completo desastre, e é exatamente esse tipo de situação o que está ocorrendo no Brasil pois a alta tecnologia alinhada à inteligência artificial reporta à escalabilidade e isso significa dizer que quanto o maior número de dados pessoais inseridos nesse sistema, maior a capacidade de acuracidade que este algoritmo tem de identificar e traçar o perfil do indivíduo. Por isso, o profissional e operador do direito, principalmente, deve conduzir a implementação do "Programa de C*ompliance* LGPD do Brasil" que garantam que os direitos fundamentais não fiquem apenas como direitos presentes na Carta Magna, principalmente que coloque a LGPD em prática, tornando assim o sistema empresarial mais sadio para atender as necessidades da sociedade, em primeiro lugar, do que os seus interesses particulares sobre o interesse público.

Apesar dessa legislação trazer a possibilidade e até o dever de anonimização[88], em alguns casos, há a possibilidade de engenharia reversa, ou seja, situação que o cientista de dados consiga por um caminho inverso ao da aplicabilidade inicial da inteligência artificial, em determinado tratamento que tornou o dado anonimizado, consiga por meio dessa estratégia, reverter a ordem matemática e desconstruir a

[88] *Dado anoninimizado é dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento – III,* art. 5º da Lei 13.709/2018.

anonimização; chegando assim um ponto de descoberta identificável, ou pessoa identificada.

Perceba que a figura do advogado é demasiadamente importante em todos os processos, porque antes da contratação inicial de uma empresa a determinado cliente ou na compra ou uso de determinada tecnologia, faz-se necessário ajustar todos esses detalhes o que são extremamente importantes, igualmente, para a proteção dos dados pessoais do indivíduo final do qual receberá o tratamento, já que o advogado deve assegurar em cláusula contratual que fica vedada a engenharia reversa, pois esse assunto é lacuna da Lei Geral de Proteção de Dados Pessoais, pois ela somente menciona em seu 12º artigo[89] a reversão para dizer se é ou não dado pessoal, mas não trata de ajustar prováveis acontecimentos e prever sobre penalidades quando de sua ocorrência.

Acredita-se que o principal cerne da LGPD, além de ser a adequação e regulamentação sobre a proteção dos dados pessoais, é trazer ao indivíduo a informação sobre o meio como o seu dado é tratado, e determinar direitos inerentes sobre ele, que serão tratados adiante; e até mesmo informações básicas como se há cadastro em seu nome em

---

[89] **Art. 12**. *Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.*

*§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.*

*§ 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.*

*§ 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.*

determinada empresa[90], e é aí, neste último trecho, que se encaixa a figura do consentimento.

O consentimento é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada[91]; o que significa entender que qualquer empresa que tiver em sua base de dados pessoais informações relativas a determinado indivíduo, terá te ter o o*pt-in* do titular do dado, ou no suprimento do consentimento por uma das bases legais autorizadoras.

O *opt-in* é um termo em inglês o que é a expressa manifestação da vontade do indivíduo para determinado tratamento de dados pessoais; é a concordância sobre determinado tratamento, em contrapartida deste termo, deve obedecer a determinados requisitos, que passará a se expor no capítulo final deste trabalho.

A Lei Geral de Proteção de Dados Pessoais traz a figura de seis sujeitos, como o titular de dados pessoais, o controlador, o operador, o encarregado (DPO — *Data Protecion Officer* da GDPR), o órgão de pesquisa, a Autoridade Nacional de Proteção de Dados.

Vista toda situação histórica com os dados sensíveis, o legislador da Lei Geral de Proteção de Dados Pessoais trouxe hipóteses restritivas ao tratamento destes dados, acertadamente somente sob a hipótese de consentimento ou tratamento pelo Poder Público ou por órgãos de pesquisas, garantindo a anonimização desses dados pessoais sensíveis, ou quando não for possível, o seu tratamento de forma adequada e de acordo com esta legislação; quando quiser ou precisar fazer uso regular do direito quanto a esses dados pessoais, para

---

[90] Apesar da lei geral de proteção de dados pessoais trazer a responsabilização para autônomos que também tratem dos dados pessoais com retorno financeiro e as específicas ações taxativas trazidas em lei, este trabalho se reduz a mencionar as obrigações às empresas. Portanto, qualquer leitura que o leitor fizer quando essa mestranda fala sobre empresas, ele pode entender também que os autônomos se encaixam nesse perfil.

[91] Art. 05º, XII da Lei 13.709/2018 (VADEMECUM SARAIVA, 2020).

assegurar a proteção à vida ou a incolumidade física do indivíduo ou de outro que esteja envolvido no caso concreto; para tutela de saúde quando houver necessidade de realizar algum tratamento médico ou por qualquer profissional da área da saúde ou de autoridade sanitária; ou ainda, para prevenção de fraude ou segurança do indivíduo nos processos de identificação e autenticação em aparelhos eletrônicos.

A Lei Geral de Proteção de Dados Pessoais trouxe ao indivíduo o exercício do direito de confirmar em qualquer empresa, se existe um cadastro interno em seu nome, ter acesso à eles, inclusive, com todos os dados e informações pessoais referentes à essa pessoa, para se objetivar a correção, atualização, inclusão de seus dados pessoais, inclusive a ter o direito de eliminar qualquer dados excessivos, ou simplesmente que o titular do dado não queira exibi-los, desde que essa empresa não seja obrigada pela legislação a armazenar por um certo período de tempo esses dados pessoais.

Isso significa dizer que, àquela empresa chata que liga insistentemente e que você já pediu centenas de vezes que ela exclua seus dados do banco de cadastro, mas, mesmo assim, ela continuou importunando você, a partir de agora, caro leitor, você pode então, pedir que essa empresa se explique, e além do dano moral ensejado, o titular de dados pessoais poderá pedir reparação ou explicações das quais ele também será multado pelo tratamento indevido dos dados pessoais.

Apesar da LGPD ter tido dois anos de vacância para que as empresas pudessem se adequar, vários projetos de Lei tentaram impedir a sua entrada em vigor, sobretudo no ano de 2020; já buscavam fundamento para isso. Tendo em vista o tempo proximal da vigência, mais de 80% das empresas ainda necessitavam se adequar[92]; mas nem a pandemia foi capaz de deter a sua força, que não vem de 2018, mas desde 1789.

---

[92] Revista Época Negócios. Tecnologia. Disponível em: <https://epocanegocios.globo.com/Tecnologia/noticia/2019/11/84-das-empresas-brasileiras-nao-estao-preparadas-para-lgpd.html>. Acesso 22/06/2021.

Com tanta pressão política houve um desfecho positivo em 18 de setembro de 2020, e a LGPD tão menosprezada pelas empresas, já é realidade, está em vigor; e a partir 01º de agosto de 2021, a Autoridade Nacional de Proteção de Dados Pessoais poderá aplicar as sanções pelo seu descumprimento. Dentre elas estão, advertência com o prazo para que as empresas adotem medidas corretivas quando o tratamento de dados pessoais for realizado indevidamente; multas que variam de 2% do faturamento do último exercício da empresa declarado no imposto de renda até R$ 50.000,00 (cinquenta milhões de reais) por infração[93]; o bloqueio e/ou eliminação de dados pessoais até que essa infração seja então sanada; a suspensão parcial, total ou proibição do exercício da empresa realizar tratamento nos dados pessoais; e por último a publicização da infração pela empresa[94].

Propositadamente, a publicização da informação de que a empresa infringiu as regras impostas pela Lei Geral de Proteção de Dados Pessoais, ficou por último porque, acredita-se que esta pena é a maior das penalidades trazidas como sanção quando houver infração desta Lei por parte das empresas. Acontece que, a era da imagem e da sociedade de dados trouxe consigo a exaltação do bem-estar das pessoas quanto as empresas em que elas trabalham e das pessoas quanto a empresa quais elas dirigem. Esse entendimento se teve após

---

[93] **Art. 52**. *Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: [...]*

*II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração.* [...]

[94] **Art. 52**. *Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: [...]*

*IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência.* [...]

funcionários da Cambridge Analytica, qual faziam parte do *head* de operações, liderando os grandes projetos quanto a análise dos dados pessoais das pessoas informações publicadas em suas redes sociais ponte, isso significa entender que quando esses profissionais denunciaram a própria empresa.

Por meio dos depoimentos desses ex-funcionários, ficou claro que passaram a ter nojo de como eram tratados os dados pessoais na empresa onde eles trabalhavam, porque o titular do dado pessoal, sequer, tinha conhecimento de como eram realizadas as análises dos perfis dos usuários nas redes sociais.

Fica muito evidente que a imagem da empresa virou a alma do negócio, por isso que as multinacionais evitam que ela seja manchada. Desta forma, a Autora busca trazer, necessariamente o que deve ser feito objetivamente para que atos preventivos sejam realizados, objetivando obstar essa infração que é a mais temida pelas empresas; não sendo possível, ter tomado medidas que sirvam de parâmetro e critério na avaliação da dosimetria da pena a será aplicada nas empresas, o que será visto e tratado no próximo capítulo.

Em 2019, a Edição da Lei Complementar 166/2019 que alterou a Lei Complementar 105, trazida acima, a Lei 12.414/2011[95], muda para sistema *opt-out* e altera substancialmente a norma, dando a opção da pessoa entrar (sistema *opt-in*) e sair do cadastro, quando entender cabível; esta alteração imputou maior responsabilidade quanto a prévia informação ao indivíduo sobre a identidade do gestor, o armazenamento de dados pessoais e a finalidade dos dados, que é exatamente traços marcantes da Lei Geral de Proteção de Dados Pessoais.

---

[95] Lei nº 12.414, de 09 de Junho de 2011. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>. Acesso 22/06/2021.

Para finalizar a linha do tempo, acrescenta-se o Decreto Lei n. 10.474 de 2020[96] que aprovou a criação da Autoridade Nacional de Proteção de Dados, proporcionando maior robustez de conscientização às empresas, no sentido de coação mesmo, pois desta forma imperativa, a LGPD tem mais respeito para exercer o seu papel de proteção dos dados pessoais dos indivíduos.

Quadro Geral de Gerações:

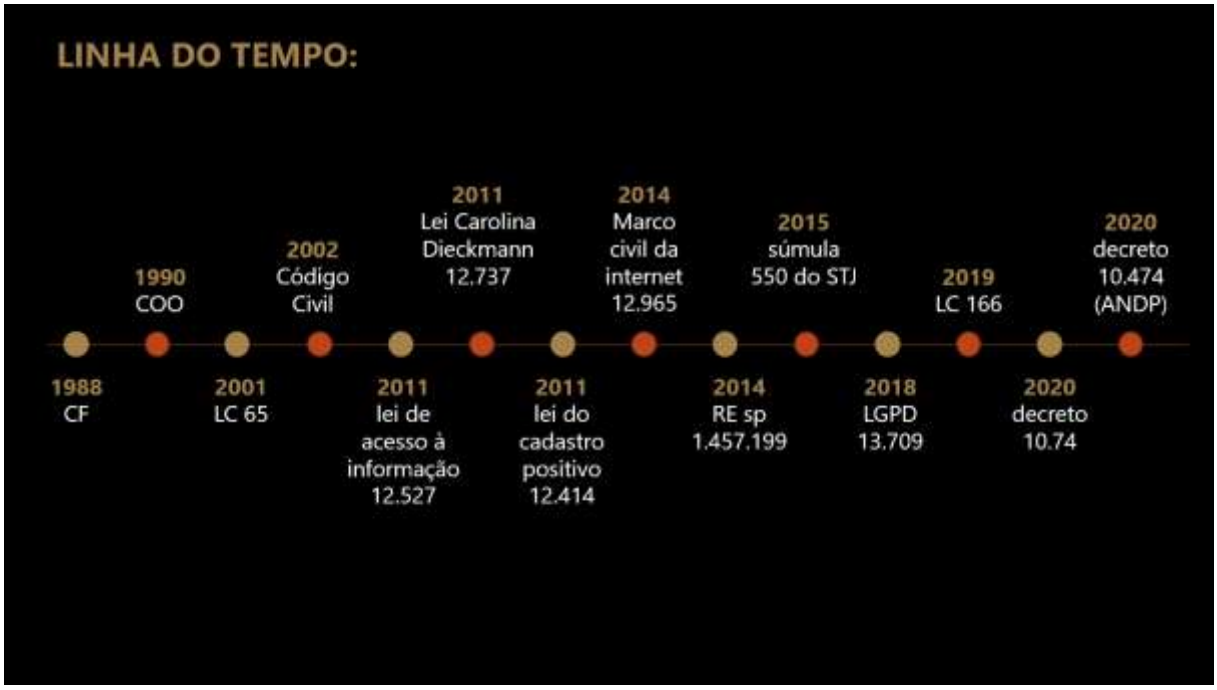
| |
|---|
| 01ª Geração: Caso *National Data Center* – EUA – o foco era no banco de dados e não na privacidade na década de 70. |
| 02ª Geração: Constituição de Portugal, Espanha e Áustria. Percepção da liberdade individual negativa – Lei da Áustria e da França (1978). |
| 03ª Geração: decisão do Tribunal Constitucional Alemão que criou o termo direito de autodeterminação informativa ou informacional – 1983, da participação mais ativa do cidadão no tratamento de seus dados. |
| 04ª Geração: Laura Mendes. As normas gerais de proteção de dados devem ser complementadas por normas setoriais. |
| Proibição de tratamento de dados sensíveis. |

Para acompanhar melhor esta evolução, separa-se as principais legislações acerca do tema em comento, em forma de linha do tempo[97], conforme se pode ver:

[96] Decreto nº 10.474, de 26 de Agosto de 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10474.htm. Acesso 22/06/2021.

[97] Linha do tempo construída pela Autora de acordo com as pesquisas cientificas realizadas sobre os levantamentos das legislações pertinentes ao tema deste trabalho.


LINHA DO TEMPO:
1789
declaração de Direito do Homem e do Cidadão
1890
artigo de Samuel Warren e Louis Brandeis
1948
declaração universal dos direitos humanos
1950
convenção europeia de direitos humanos
1957
tratado sobre o funcionamento da União Europeia dados pessoais
1963
protocolo 4 convenção europeia de direitos humanos
1981
convenção do Conselho da Europa Estrasburgo
1995
diretiva 95/46/CE (Dados Sensíveis)
2008
regulamentos CE 1338 do Parlamento europeu e do Conselho
2016
regulamento 2016 679 (GDPR)


LINHA DO TEMPO:
1988
CF
1990
COO
2001
LC 65
2002
Código Civil
2011
lei de acesso à informação 12.527
2011
Lei Carolina Dieckmann 12.737
2011
lei do cadastro positivo 12.414
2014
Marco civil da internet 12.965
2014
RE sp 1.457.199
2015
súmula 550 do STJ
2018
LGPD 13.709
2019
LC 166
2020
decreto 10.74
2020
decreto 10.474 (ANDP)

# 3 COMO AS EMPRESAS DEVEM REAGIR À NOVA SOCIEDADE DE DADOS?

As empresas devem recepcionar a Lei Geral de Proteção de Dados Pessoais como uma nova chance de se alterar, até se for necessário, o seu *status quo* (cultura), pois de fato, as empresas que necessitam terão estrutura que vai originar a proteção de dados pessoais do indivíduo; já que é comumente visto que há empresas no Brasil sequer possuem estas bases para serem atualizadas e adequadas à LGPD. Desta forma, essas empresas necessariamente necessitam de profunda alteração que lhes confira a eficácia de um planejamento para receber a estrutura de uma nova ordem de proteção de dados pessoais que confira proteção aos dados pessoais de seus colaboradores, de seus funcionários, de seus prestadores de serviços, de seus clientes e de qualquer pessoa ou empresa que ele mantenha acesso a repercutir no tratamento de quaisquer dados pessoais.

Olhando ao passado, os cadernos amarelos, aqueles que traziam listas com os nomes completos das pessoas que detinham a propriedade de linhas telefônicas, inclusive com o seu endereço e o número de seu telefone nesta lista, o que ocorria em 1990, e era totalmente livre a circulação desses dados pessoais e que mesmo que se esses indivíduos titulares desses dados procurassem obstar esse tipo de ocorrência, nada podiam fazer, pois era o que se acontecia naquela década.

Atualmente, há um cenário bem diferente, até porque a ciência, a tecnologia e a inovação trouxeram escalabilidade para esse tipo de acesso aos dados pessoais e que pelo número incontável de pessoas a terem acesso a esses dados e informações pessoais, seria completamente avesso se permitir esse acontecimento sem o consentimento do proprietário dos dados pessoais.

Antigamente[98], parte das empresas que cadastravam os dados pessoais dos indivíduos tratavam deles como se delas fossem, que apesar do cadastro e da tecnologia utilizada para inserção e armazenamento desses dados ser da empresa, ressalta-se que os dados são da pessoa que lhes confere[99].

Apesar da Constituição federal de 1988 em seu artigo 5º, XIV[100], trazer autorização para consulta e acesso ao cadastro de dados pessoais do indivíduo, de forma gratuita, pois são atos necessários ao exercício da cidadania, esse acesso o que é direito trazido pela carta magna era somente postulado judicialmente, por meio de *habeas data,* permite a visualização e retificação de dados em registros ou bancos de dados somente pela negativa de entidades governamentais ou de caráter público, que não apresentassem espontaneamente o pedido feito pelo titular de dados. Se este pedido já era negado, tendo como direito garantido na Constituição Federal e até ação judicial necessária para a sua consecução, ademais realizar qualquer ato neste sentido pelo titular de dados que quisesse, terá acesso aos seus dados pessoais junto às instituições privadas, o que era extremamente difícil; isso só seria possível por meio de socorro judiciário.

Essa postura primata deve ser completamente extirpada da cultura das empresas, a fim de se trazer ao titular de dados uma nova

---

[98] Estude de campo da Autora na análise dos mais de 13 anos de atuação na área jurídica.

[99] **Art. 5º**. *Para os fins desta Lei, considera-se:* [...]

*I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável*. [...]

[100] **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:* [...]

XIV - *é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional.* [...]

experiência com a empresa ao qual ela lhe confiará os seus dados, e assim, criar esperança, uma realidade protegida e segura em que o titular do dado lhe confiará essas informações. Neste sentido, o antropólogo de Dieter Wyss faz uma análise entre o NDA (*Non Disclosure Agreement)* e sobre a relação de realidade e confiança entre as pessoas, o significado trazido por ele da palavra confiar traz a monta que o titular do dado espera confiança à empresa em que ele lhe passe os dados. Confiar significa: entregar-se à proteção de alguém ou algo (coisa, instituição, natureza etc.), por si à mercê de outro, seja a pessoa ou coisa[101].

Empresas devem agir também de forma a não somente acatar o cumprimento da Lei Geral de Proteção de Dados Pessoais, a Constituição Federal, ao Marco Civil da Internet, a Lei de Acesso à Informação, ao Código de Defesa do Consumidor, a Lei Carolina Dickman, mas sobretudo, obstar atos de seus colaboradores que condicionem a violência simbólica; aquele ato que normalmente encontra-se entre linhas, pois é dificilmente perceptível aos olhos de terceiros, mas facilmente percebido pelos olhos da vítima, ou seja, do titular do dado que se viu numa situação discriminatória, tendo em vista algum dado pessoal sensível atinente à sua pessoa, por exemplo.

O termo "violência simbólica" foi usado pelos sociólogos franceses Pierre Bourdieu e Jean Claude Passeron[102], na década de 70, para expressar sobre atos de indivíduos agressores neste mesmo sentido, difíceis de serem vistos por terceiros, porque esta violência é praticada por meio de símbolos, ou seja, pode ser por meio de linguagem corporal, por meio de expressão facial, e que estas são produzidas em

---

[101] SANTOS, Maria Celeste Cordeiro Leite dos. **Poder Jurídico e Violência Simbólica**. 1ª Ed. São Paulo: Editora Cultural Paulista, 1985. p.137.

[102] Informação obtida nas aulas de Teoria Geral do Direito no segundo semestre de 2017 com a Professora Maria Celeste Cordeiro dos Santos, crédito para obtenção do Mestrado em Filosofia do Direito junto à PUC/SP.

milésimos de segundos, mas chegam à alma da vítima e provocam sérios problemas de saúde mental.

Busca-se reforçar sobre a violência simbólica neste trabalho, sobretudo neste título, de como as empresas devem reagir a uma nova sociedade de dados porque a massificação do tratamento de dados pessoais remonta a um intenso trabalho em escala da qual essa empresa passará a trabalhar e o advogado a produzir mediante os novos costumes da era da sociedade de dados, e com o iniciar disso, os colaboradores que deterão o poder de ter acesso à esses dados e informações pessoais deverão ter cautela em suas profissões, e as empresas são responsáveis por isso.

Já ciente que a violência simbólica está conectada com o poder e este com o controle, dessa forma, faz-se uma análise do pensamento da filósofa Maria Celeste Cordeiro Leite dos Santos de que a violência simbólica na verdade se utiliza de outro instrumental do poder e que ela tem, ou seja, uma força duplicada pelo próprio poder que é uma violência que lhe impõe.

E essa força pode ser percebida pela conclusão do pensamento de Pierre Bourdieu e Jean Claude Passeron quando eles afirmam que todo o poder de violência simbólica, isto é, todo o poder que chegar por significações e impô-las como legítimas, dissimulando as relações de força que estão na base de sua força, acrescentam à sua própria força, isto é, propriamente simbólica, tais relações de força[103].

A filósofa também faz uma reflexão interessante sob a visão de Tércio Sampaio Ferraz Júnior, em que ter poder aplicado a uma violência simbólica faz com que a vítima seja neutralizada, a ponto de permanecer imóvel, isso significa entender no campo da proteção de dados pessoais, olhando para todo o cenário histórico de poder, controle e violência praticados a determinados grupos de indivíduos, em razão desses dados pessoais sensíveis, que o detentor do poder aliado à prática de discriminação quanto aos dados pessoais, seja principalmente, por

---

[103] SANTOS, Maria Celeste Cordeiro Leite dos. **Poder Jurídico e Violência Simbólica**. 1ª Ed. São Paulo: Editora Cultural Paulista, 1985. p. 151 e ss.

dados pessoais sensíveis, que são eles sobre a sua 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[104] quem é o detentor do poder e controlador dos dados pessoais leva o titular do dado a uma relação de poder da qual ele é neutralizado e fica impotente de realizar qualquer tipo de defesa neste cenário de violência simbólica. Como foi o caso de vários eventos ocorridos no passado e trazidos à baila neste trabalho, no primeiro capítulo, em que foi destacado alguns acontecimentos de extrema violência e morte no âmbito mundial.

Com essa reflexão, é possível compreender o que de fato ocorreu no passado e analisar a relação de poder, por exemplo, entre Hitler e o povo judeu, da qual ele exterminou, em razão de sua origem, simplesmente pela nacionalidade; o que é um completo absurdo, pois o indivíduo não escolhe a nacionalidade, ele não escolhe ter nascido em determinado país ou ser originado de certa família. É completamente imoral excluir uma classe de indivíduos pela sua nacionalidade e muito menos matá-los por esse motivo torpe. O acesso que teve Hitler sobre a moradia desses judeus e onde eles estavam localizados, aliado ao poder de mando fez com que esses judeus que estavam neutralizados pela força da violência simbólica que tinha Hitler caminhassem para a sua própria morte, sem que houvesse qualquer coação envolvida no sistema, pois eles acreditavam que aquela cidade seria separada para a raça deles. E, olhando para o passado desta maneira, entende-se quando Maria Celeste Cordeiro Leite dos Santos e Tércio Sampaio Ferraz Júnior afirmam que quando é necessário aplicar a coação a determinado indivíduo é porque ali o poder já se acabou, é porque esse poder foi reduzido a zero. Portanto, perceba, o poder incontestável de Hitler presente e muito forte, para sequer, utilizar do artefato de coação para que os extermínios ocorressem.

---

[104] Art. 5º, II da Lei 13.709/2018.

Aos judeus foram aplicadas a violência simbólica em “pílulas” que os levaram a sua morte, por isso, as empresas têm o dever de inibir qualquer ato de violência simbólica de seus colaboradores e deve trazer esse espírito no regulamento interno para que fique claro e transparente que atos como esses que ocorreram no passado e continuam acontecendo de outra maneira sejam frustrados pelas regras e políticas internas de uma empresa que respeita, preserva, e acima de tudo, honra a vida humana e ao seu próximo, que entre todos os mandamentos das Leis de Deus é o segundo mais importante, só ficando atrás do mandamento em que é preciso amar a Deus acima de todos e todas as coisas, e esse segundo mandamento é semelhante a este primeiro ame o seu próximo como a ti mesmo.[105]

E é transmitir exatamente esses valores de exaltação da vida humana e proteção aos seus direitos que lhes são inerentes como os direitos fundamentais e os direitos humanos, que a empresa precisa mostrar a sua preocupação com o seu próximo, e estes próximos nada mais são do que os seus colaboradores, do que os seus clientes, os seus fornecedores e os seus parceiros; além de ser uma ótima ideia para o *marketing* e que por consequência precisa ter bem definidos para a expansão de sua marca, de seus produtos ou de seus serviços, os valores, a missão e a visão moderna e atualizada que a empresa tem deste novo mundo e desta nova era da sociedade de dados.

As empresas devem demonstrar à sociedade que a Lei Geral de Proteção de Dados Pessoais não é somente uma simples e pura adequação de normas, de regras para se objetivar a proteção de dados pessoais, é o exercício regular do direito a fazer exercer as liberdades dispostas na Lei 13.709/2018 quanto aos seus dados pessoais, contudo, é a própria alteração na cultura interna da empresa; é o enfoque de se ligar ao direito natural do ser humano.

Apesar da sociedade de dados trazer um distanciamento social, que foi elevado em razão da pandemia provocada pelo novo Coronavírus,

---

[105] Mateus 22:39 (DANTAS, Maria Augusta. **Bíblia Revisitada para Jovens**. Campinas: Bookseller, 2020).

as empresas devem dar o tratamento adequado, não só pela sua obrigação legal e moral com o Estado e com o titular do dado, mas pela empatia ao lidar com esse assunto que aparentemente tão simples, mas que traz um plano de fundo manchado de sangue, de ódio e de muita violência.

Os colaboradores, os funcionários, os clientes, os prestadores de serviços, os fornecedores, e a sociedade como um todo precisam conhecer essa nova cultura das empresas, pois de fato, publicizar a nova filosofia da empresa e para algumas poderia escrever uma nova história, e para outras continuar essa linda história da empresa.

Diante do poder e controle vistos anteriormente nos capítulos escritos acima, de terror e pranto margeado à eles, este trabalho, diante desta problemática em escala, propõe trazer as empresas (detentoras do poder) a visão para que trabalhem o poder como meio de comunicação[106], que seria uma teoria do poder como meio de comunicação estudada por Niklas Luhmann e Tércio Sampaio Ferraz Júnior, trazida neste livro pela leitura dos reflexos escritos da filósofa Maria Celeste Cordeiro Leite dos Santos e que se buscou trazer para este trabalho, pois é desta forma, visão e utilização do poder por meio da comunicação, o avesso dos atos sanguinários do passado; isso se faz crer que há uma esperança em utilizar de símbolos em linguagem, o que são elementos milenares para se trabalhar com um mundo futurístico, inovador e tecnológico desta nova era.

Apesar do desenvolvimento tecnológico e da inovação serem elementos principais desta nova era e até ser fundamento da LGPD, a empresa necessita do meio de comunicação mais antigo para se fazer valer da eficácia e o poder que a comunicação tem, pois, sem o poder e controle, nada adianta do uso da força e de maneiras coercitivas puramente sozinhas, claro que esses meios de punição devem estar presentes. No entanto, não serão o imperador para um manejo com o *compliance* da proteção de dados pessoais, isto porque, a força - o uso

---

[106] SANTOS, Maria Celeste Cordeiro Leite dos. **Poder Jurídico e Violência Simbólica**. 01ª – São Paulo: Editora Cultural Paulista, 1985. p. 156.

concreto, alcança muito rapidamente o seu ponto de esgotamento como condição do poder: para vencer uma luta, força decisiva, mas não para manter o poder[107].

No campo profissional, na labuta diária em implementar o "Programa de *Compliance* LGPD do Brasil", essa Autora encontrou muita dificuldade em explicar sobre esta nova Lei de proteção de dados pessoais, até porque, algumas empresas só conseguiam enxergar gastos, e não investimentos e dever legal. Nesta sociedade de dados o que é preciso ser feito para estar em consonância com a Lei brasileira, dificuldade essa encontrada desde 2019 e 2020 primeiro semestre, porque a Lei Geral de Proteção de Dados Pessoais não estava vigorando em sua maioria dos artigos.

Quando se mencionava em consultorias e reuniões[108] que os artigos das sanções administrativas estavam sob *vacatio legis*, demorava-se a marcar outro encontro para a apresentação de proposta do "Programa de *Compliance* LGPD do Brasil" e de honorários advocatícios, que, apesar das sanções revelarem-se pesadas, dentre elas advertência, multa de até 2% do faturamento da empresa declarado no seu último imposto de renda e limitada a R$ 50.000.000,00 (cinquenta milhões de reais) por infração, de ter multa diária neste importe, da infração da empresa, ser levada a publicização em mídia, de haver bloqueios de dados pessoais até que sejam adotadas medidas corretivas desta infração, da eliminação de dados sobre essa infração, da suspensão parcial ou total do tratamento de dados pessoais, exatamente porque, as empresas com essa atitude demonstravam que não estavam se importando, de fato, com a proteção de dados dos indivíduos, mas sim, com os seus próprios cofres e interesses particulares, sem qualquer atenção aos direitos do próximo.

---

[107] SANTOS, Maria Celeste Cordeiro Leite dos. **Poder Jurídico e Violência Simbólica**. 1ª Ed. São Paulo: Editora Cultural Paulista, 1985. p. 159.

[108] Estudo de campo trazido pela experiência corrente da Autora no trabalho jurídico atuado na Advocacia Baccari.

Como em meio a todos esses anos, desde que a Lei Geral de Proteção de Dados Pessoais foi sancionada em 14/08/2018, foram apresentados vários projetos de Leis que tentaram postergar a vigência da Lei; as empresas estavam em um cenário bem confortável, pois a maior parte delas não acreditavam que a sua eficácia plena chegaria ao seu alcance em 2020.

Isso porque desde o início quando o presidente da República Michel Temer, então na época, sancionou a Lei Geral de Proteção de Dados Pessoais, já havia a previsão de vacância da Lei durante 24 meses após a sua publicação[109]. Período até que adequado para que houvesse atualização para a recepção desta nova Lei — o que é extremamente específico sobre a proteção de dados pessoais.

O que se esperava das empresas com a chegada da LGPD no Brasil era uma atualização em seu cenário do mapeamento de dados pessoais, já que existiam Leis brasileiras com margem para interpretação jurídica em seu campo geral que poderia permear regramentos sobre os tratamentos de dados pessoais, até porque uso da tecnologia já vem sendo explorado desde 1970 no laboratório de microeletrônica da USP, inclusive um dos fundadores deste laboratório é doutrinador João Antônio Zuffo[110].

Nesta esteira, faz se repousar que as empresas, em sua grande parte, iniciariam esse processo regulatório quando, de fato, houvesse

---

[109] **Art. 65**. *Esta Lei entra em vigor: (Redação dada pela Lei nº 13.853, de 2019) [...]*

~~*II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos. (Incluído pela Lei nº 13.853, de 2019)*~~

~~*II - em 3 de maio de 2021, quanto aos demais artigos. (Redação dada pela Medida Provisória nº 959, de 2020) (Convertida na Lei nº 14.058, de 2020)*~~

*II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos. (Incluído pela Lei nº 13.853, de 2019)*

[110] ZUFFO, João Antonio. A Infoera: O Imenso Desafio do Futuro. São Paulo: Editora Saber Ltda., 1997.

intervenção política, e foi o que ocorreu na quinta-feira do dia 17/09/2020, quando o presidente Jair Bolsonaro Sancionou a LGPD e que em tão passou a ter eficácia plena a partir da sua publicação que ocorreu em 18 de setembro de 2020. O que fez com o que as empresas exteriorizassem, então a sua preocupação com a nova Lei Geral de Proteção de Dados Pessoais e essa postura remonta ao pensamento do filósofo Márcio Pugliesi, o criador da denominação sociedade de dados:

> O habitante da cidade preocupa-se com seus próprios problemas e nada faz em relação à infração de regras a não ser que ela interfira em seus negócios[111].

No entanto, vale dizer que nesta caminhada profissional da Autora que vos fala, no assessoramento e implementação do "Programa de *Compliance* LGPD do Brasil", uma pequena parcela de empresas[112] se preocupou desde o início em que a Lei Geral de Proteção de Dados Pessoais foi sancionada.

Foi possível acompanhar dessa pequena parcela de empresas que os seus diretores CTO (*Chief Technology Officer*), estavam de fato querendo se adequar a LGPD e a proteger os dados dos indivíduos, inclusive pautados na transparência, que é um dos princípios que lei determina em conjunto com a boa-fé, dentre outros princípios estão o princípio da finalidade da adequação, da necessidade, do livre acesso, da qualidade dos dados, da segurança, da prevenção, da não discriminação, e da responsabilização e prestação de contas aos titulares de direito.

E, por incrível que pareça, por experiência de campo, 100% das empresas que procuraram esta autora para prestar consultoria sobre

---

[111] PUGLIESI, Márcio. ***Filosofia Geral e do Direito****: uma abordagem sistêmico-construcionista.* Chisinau: Novas Edições Acadêmicas, 2021, p.753.

[112] Estatística realizada com os clientes que procuraram a Advocacia Baccari sobre o tema e dentro os clientes já com assessoria jurídica empresarial sobre outros naturezas que foram comunicados a respeito da nova Lei 13.709/2018, do primeiro semestre de 2019 até 22/06/2021.

proteção de dados pessoais é do setor de tecnologia, ou seja, alguém ligado à criação de algoritmos, da produção de inteligência artificial, da segurança da tecnologia da informação, do *business intelligence*.

E esse interesse pelos profissionais da tecnologia da informação e da produção, desenvolvimento e aplicação da inteligência artificial, não são avulsos, já que, a Lei Geral de Proteção de Dados Pessoais traz uma certa responsabilização para os profissionais da segurança, imputando-lhes a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e ações acidentais ou ilícitas de destruição, perda, alteração comunicação ou de fusão[113], assim como traz a responsabilização e prestação de contas como a demonstração, pelo agente da adoção de medidas eficazes capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais é, inclusive, da eficácia dessas medidas[114], ou seja, a lei traz figuras bem desenhadas das quais participarão obrigatoriamente desse processo de adequação e que principalmente dentre as pessoas que comporão a equipe do setor de controle de dados pessoais, estarão o controlador, o operador e o encarregado.

Na pragmática, normalmente este profissional da tecnologia e da inteligência artificial é o chamado controlador e o operador, pois o controlador é a pessoa que chefia e toma as decisões que deverão ser realizadas pelo operador, o que normalmente ocorre é que o operador é o cientista de dados, um criador de algoritmos, de *softwares*, o que produz os códigos, as ferramentas, os instrumentos desta tecnologia, liderados e supervisionados certamente por outro profissional mais gabaritado, capacitado e experiente, mas que também é da tecnologia ou da inteligência artificial, quando envolve empresas do seguimento de tecnologia e inteligência artificial.

---

[113] Art. 6º, VII, da Lei 13.709/2018.

[114] Art. 6º, X, da Lei 13.709/2018.

Os criadores das novas tecnologias ou os que também utilizam as ferramentas de produção em escala da inteligência artificial produziam essas tecnologias bem distantes do profissional regulador das leis, que é o advogado, o qual nem fazia parte da equipe multiprofissional e muito menos era chamado para participar do processo de desenvolvimento dela, mas tão somente quando da sua regulamentação ou de sua proteção contra plágios no campo dos registros de patentes.

Os profissionais desse segmento, ganharam um capítulo especial na Lei Geral de Proteção de Dados Pessoais e foi o que também os preocupou, já que a lei 13.709 de 2018 trouxe determinações expressas de que eles devem respeitar algumas obrigações impostas pelo legislador[115] e que isso também não lhe custa somente mão-de-obra para tanto, já que as máquinas farão este trabalho, mas que dependendo da cultura anterior da empresa e até do capital que ela destina de investimento quanto aos registros de dados pessoais dos titulares, devem gravar os logs, elaborar relatórios de impactos quanto à proteção de dados pessoais, principalmente sensíveis, obedecer firmemente o regulamento interno e seguir à risca as políticas de governança e de privacidade, pois mesmo se ocorrer um evento danoso, terão o manual de boas práticas para serem conduzidos.

Então com esse capítulo todo especial dedicado ao controlador e ao operador, principalmente, a partir da Lei Geral de Proteção de Dados Pessoais trouxe consigo direitos e ressarcimento quanto aos danos causados aos proprietários dos dados pessoais, o que era visto como penalização às empresas. Com a chegada da LGPD no Brasil, passou a se responsabilizar não apenas a pessoa jurídica e o seu

---

[115] **Art. 50**. *Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.* [...]

conseguinte CNPJ, mas agora a lei traz em seu bojo a responsabilidade do profissional com o seu CPF, aquele operador ou controlador responsável pelo tratamento dos dados pessoais e destas informações relacionadas à pessoa. Desta forma, deverão também reparar o dano como pessoa física, de acordo com a mitigação de suas responsabilidades.

Assim, fica claro entender o motivo pelo qual leva esses profissionais, principalmente da área de tecnologia da informação, desenvolvimento, e de inteligência artificial, a se preocuparem em primeiro lugar com a LGPD, pois eles responderão solidariamente[116] pelos danos causados aos titulares de direito caso não haja um contrato que defina muito bem as atividades e os deveres da operação, e pela falta de clareza, a advertência será uma das penalidades que a Autoridade Nacional de Proteção de Dados poderá notificar a prestar esclarecimentos.

Contudo, é necessário ponderar que a figura do advogado não se limita a apenas confeccionar e revisar disposições contratuais, pois por si só, não afastarão a responsabilidade civil e criminal do operador e do controlador, no caso de responsabilização e reparação do dano, principalmente quando houver auditoria por parte da Autoridade. Os

---

[116] **Art. 42**. *O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. [...]*

*§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:*

*I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;*

*II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei. [...]*

documentos servem para formalizar os atos da rota de *complince*, por isso, é extremamente necessário o controle e supervisão desta implementação, para prevenir incidentes e ventos, inclusive para apurar de fato o infrator, que será explanado adiante.

A fiscalização poderá ser avulsa por parte da Autoridade Nacional de Proteção de Dados Pessoais, pelo próprio Titular do dado, por meio de uma denúncia, por exemplo, direcionada à entidade, sendo no âmbito administrativo. Por parte de patronos, representando um operador, um controlador, ou um titular, em uma notificação extrajudicial direcionada a algum dos sujeitos da atividade, ou mesmo incluindo a própria Autoridade Nacional de Proteção de Dados para que o assunto seja resolvido na esfera de resolução de conflitos alternativos por meio de uma câmara arbitral. E em última análise, ou mesmo abreviando caminhos, caso a linha de trabalho do patrono seja mais combativa, e não havendo causas de anulação para se ingressar direto junto ao Poder Judiciário, a distribuição de ação judicial poderá resultar, além das sanções previstas no artigo 52 da Lei 13.709/2018, será cumulada multa diária por descumprimento de decisão/sentença judicial e/ou indenização por dano moral, como ocorreu no caso da CYRELA.

A ação judicial do caso “Cyrela” (Processo número 1080233-94.2019.8.26.0100)[117] repercutiu as notícias e mídias sociais tendo em vista que o ponto nuclear do pedido foi a LGPD, desta forma, até o presente momento, a empresa foi penalizada em multa diária por descumprimento no valor de R$ 300,00 (-) e em dano moral no valor de R$ 10.000,00 (-) pela violação os fundamentos da LGPD, condutas ilícitas aos artigos 186, 187, 422 e 2.035, parágrafo único do Código Civil, pois a juíza de Direito entendeu ser a função social da propriedade intelectual e dos

[117] Tribunal de Justiça de São Paulo. Consulta Processual. Disponibilizado em: <https://esaj.tjsp.jus.br/cpopg/show.do?processo.codigo=2S0013T8I0000&processo.foro=100&processo.numero=1080233-94.2019.8.26.0100&uuidCaptcha=sajcaptcha_c26aa6fcc4db4531a00f790503d3453a>. Acesso em 22/06/2021.

contratos, disposição legal constante no artigo 170, III, da Constituição Federal[118], baliza para tratamento dos dados pessoais do Autor da ação movida, entendendo que os profissionais que possuem acesso aos dados cadastrais do cliente deveriam ter treinamento sobre sigilo e confidencialidade de dados e informações pessoais.

Por esses profissionais terem acesso privilegiados sobre a localização virtual, armazenamento eletrônico, tratamento em geral e a forma com que esses dados pessoais são tratados, deve ser obrigatoriedade das empresas quanto a promoção de boas práticas e atualização da Lei, neste sentido.

Desta forma, os colaboradores sentem-se inseguros em trabalhar em uma empresa quem não observa a legislação[119], pois não promovem a segurança adequada para a proteção dos dados pessoais do titular do dado. Se tratando de uma empresa de tecnologia ou de inteligência artificial, eles sabem o resultado e o risco que se pode ocasionar, até porque, esses profissionais, são os que também atuam na segurança da informação e com isso, sabem exatamente os pontos de vulnerabilidades do sistema, limitações que seu cargo impõe quanto à contratação de novos serviços; de certa maneira, quando não disponibiliza o capital necessário para se promover a segurança necessária, que é esperada por eles, há frustração e desapontamento.

É o colaborador deste setor que está apto a resolver os problemas quando uma máquina é infectada por um *malware* e que sabe exatamente como se faz para inibir a infestação a outros computadores, *softwares*, servidor e outros dispositivos; mas acontece que, essas regras que às vezes estão subliminarmente impostas, pela prática diária

---

[118] **Art. 170**. *A ordem econômica, fundada na valorização do trabalho humano e na livre iniciativa, tem por fim assegurar a todos existência digna, conforme os ditames da justiça social, observados os seguintes princípios:* [...]
*III - função social da propriedade.* [...]

[119] Percepção obtida nas entrevistas realizadas com colaboradores das empresas em que a Autora faz a implementação de *compliance* pela Advocacia Baccari.

do profissional, agora deverá ser colocada à vista de toda a equipe, inclusive com treinamentos e seguir à risca o manual de boas práticas para que a empresa obedeça aos critérios objetivos da lei.

Tendo uma Autoridade que vai fiscalizar os atos das empresas, elas devem reagir de uma maneira positiva quanto a essa mudança de cultura, mas que de maneira rápida tenda a criar metodologias internas que sejam efetivadas pois a Autoridade Nacional de Proteção de Dados vai aplicar sanções em decorrência do descumprimento à LGPD, e ao mesmo tempo, vai informar a população sobre os seus direitos constantes nas legislação, promovendo estudos que impactem na preservação dos direitos à privacidade dos indivíduos.

A abrangência da fiscalização da Autoridade Nacional de Proteção de Dados é ampla, pois ela poderá também solicitar informações, documentos, ações e relatórios para que a empresa comprove o seu atendimento à LGPD e, com isso, a Autoridade pode realizar auditorias e mesmo que não haja eventual desobediência à legislação, se houver qualquer incerteza jurídica, que promova dúvida quanto a proteção no tratamento de dados pessoais, a Autoridade poderá solicitar reparos à empresa.

Além disso, o Estado contará com o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade[120] que prestará serviço

---

[120] **Art. 58-B**. *Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade: (Incluído pela Lei nº 13.853, de 2019)*

*I - propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD; (Incluído pela Lei nº 13.853, de 2019)*

*II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019)*

*III - sugerir ações a serem realizadas pela ANPD; (Incluído pela Lei nº 13.853, de 2019)*

público para a sociedade e em conjunto com a Autoridade Nacional de Proteção de Dados procurará diretrizes estratégicas ou o fornecimento de subsídios para a efetiva fiscalização, elaborando relatórios, sugerindo ações, elaborando estudos, promovendo debates e audiências públicas sobre a proteção de dados pessoais e da privacidade com o intuito de promover o conhecimento sobre o tema a todos os indivíduos.

Além desses dois institutos, o Estado contará com a ajuda e o apoio, nesse sentido, do Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP)[121], o Sistema Nacional de Avaliação da Educação Superior (SINAES). O que não faltará é apoio para que haja fiscalização quanto aos deveres e acerca do que as empresas têm por imposto nesta seara, haja vista que a fiscalização será realizada; no entanto, as sanções administrativas constantes dos artigos 52, 53 e 54 da Lei 13.709/2018 só poderão ser aplicadas a partir do dia primeiro de agosto de 2021, conforme estabelecido no artigo 65, I-A[122], do supra referido diploma legal, em decorrência da Lei 14.010, de 2020, esta que dispõem sobre o regime jurídico emergencial e transitório das relações jurídicas de direito privado e no período da pandemia causada pelo novo Coronavírus, da qual editou o artigo 65 da LGPD.

Tendo as empresas, de alguma forma, que disponibilizar capital para investir na publicidade e propaganda sobre a recepção à Lei Geral

---

*IV - elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e (Incluído pela Lei nº 13.853, de 2019)*

*V - disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população.*

[121] **Art. 62**. *A autoridade nacional e o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep), no âmbito de suas competências, editarão regulamentos específicos para o acesso a dados tratados pela União para o cumprimento do disposto no § 2º do art. 9º da Lei nº 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional) , e aos referentes ao Sistema Nacional de Avaliação da Educação Superior (Sinaes), de que trata a Lei nº 10.861, de 14 de abril de 2004.*

[122] **Art. 65**. *Esta Lei entra em vigor:* [...]
*I-A – dia 1º de agosto de 2021, quanto aos arts. 52, 53 e 54.* [...]

de Proteção de Dados Pessoais e a sua adequação interna poderá promover e divulgar informações sobre esse processo, como foi o caso do Banco Santander, que foi o primeiro Banco no Brasil a criar a campanha “Santander On” para informar os seus correntistas e à sociedade sobre a sua acertada decisão em atender os parâmetros da LGPD.

A campanha Santander *On* trouxe ao consumidor o livre e gratuito acesso à corrente esta que, ao alcance de suas mãos, por meio do aplicativo do próprio banco, informa na tela todos os dados e informações pessoais que o banco tem a respeito do correntista.

Como dito anteriormente, além de cumprir com a obrigação legal, a empresa também pode utilizar desse cumprimento para realizar publicidade de ao seu favor, como inteligentemente o Banco Santander procedeu com o slogan de que é diferente das outras instituições financeiras porque eles querem uma conversa de igual para igual com o consumidor e uma nova proposta de conectar em consumidor a sua relação financeira que possui com o banco e o dinheiro movimentado em sua conta[123].

Depois desse cenário, outras empresas vieram a reproduzir eventos e publicidades também com respeito à menção de que estão se adequando à Lei Geral de Proteção de Dados Pessoais e essa exteriorização se aumentou na sexta-feira do dia 18 de setembro de 2020, quando então a lei passou a ter vigência; a maior parte das empresas correram[124] para colocar no ar um botão visível sobre política de privacidade e termos e condições de uso, especialmente quando da utilização de *cookies* para captar informações a respeito das pessoas

[123] SANTANDER. 2020. Campanha Banco Santander *On*. Disponível em: <https://www.santander.com.br/campanhas/santanderon>, com acesso em 21/09/2020.

[124] Pesquisa de campo realizada por esta Autora no trabalho profissional junto a Advocacia Baccari.

que navegam em determinado *site* ou aplicativo, como se adequar à LGPD estivesse reduzida somente à atualização desses documentos.

Outro ponto importante também, a ser trazido à baila é sobre a figura do consentimento, que será explicada, mais adiante no próximo capítulo, mas deve ser informado o que as empresas não podem resumir os seus atos impondo-lhe termos de consentimentos, o chamado *opt-in*, sem qualquer atenção aos princípios fundamentais da Lei Geral de Proteção de Dados Pessoais.

O termo de consentimento não pode ser utilizado genericamente com o pretexto de que um indivíduo autorizou a empresa a proceder com determinado tratamento nos dados pessoais, por isso, as empresas devem utilizá-lo, mas tê-lo para ser útil para ambas as partes, até porque este documento deve ser claro, objetivo, transparente e se valer de palavras fáceis para exprimir um entendimento do que o que se quis dizer ali. Nada de usar aquelas fontes minúsculas que o indivíduo precisa apertar o olho para poder tentar ler aquilo que se é exprimido.

O ponto crucial deste capítulo é que as empresas devem reagir à nova sociedade de dados sabendo que o dado é propriedade do indivíduo e não da empresa, apesar da empresa guardar o dado e necessitar dele para a execução de algum serviço ou venda de produto, o dado pessoal ainda assim continua sendo da pessoa. Acredita-se que, em razão disso, a LGPD denominou o indivíduo proprietário do dado, como “titular”[125], pois é ele quem manda e tem um poder de mando no seu dado, assim da forma como o sócio da empresa é pessoa física em algum momento da vida ele necessita de realizar o exercício de cidadania, assim se deve pensar em todas as pessoas das quais a empresa trata os dados, pois dessa maneira ele conseguirá atingir eficazmente o direito do outro já que ele pensará no outro como pensa em si mesmo.

---

[125] **Art. 5º**. *Para os fins desta Lei, considera-se:* [...]

*V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.* [...]

## 3.1 O Futuro da Tecnologia à Serviço da Proteção de Dados Pessoais

O avanço tecnológico acelerado da tecnologia não permitiu que o Direito a acompanhasse, como visto nos outros capítulos, a proteção de dados pessoais trazidas pela legislação não foram suficientes para se trazer segurança jurídica às criações no campo da tecnologia e da inteligência artificial.

O que era visto somente nos videogames e nos filmes de ficção, há muito que se tornou realidade, e veio à tona durante esta pandemia pela intensidade da utilização de aparelhos eletrônicos e digitais. Veja-se que, a empresa de inteligência artificial contou sobre a sua criação e ao mesmo tempo mostrou certa animosidade com o GPT-3[126], tido como modelo de linguagem muito poderoso, por ser um instrumento que reproduz a linguagem humana é o tal do *machine learning*, no qual ele tem 175 bilhões de parâmetros de uma rede neural com diversos modelos de linguagem. Essa ferramenta é capaz de criar textos automaticamente, o que é assustador até para o próprio CTO da Oculus VR. Essa ferramenta também tem a intenção de melhorar os *chats boots* e torná-los mais humanizados já que esta ferramenta representa um grande passo em tudo o que já foi criado na inteligência artificial.

Os aprendizados das máquinas com as informações que o ser humano insere são completamente inesperados, pois as máquinas aprendem com as próprias máquinas, ou seja, elas aprendem o que o ser humano ensinou e a própria máquina a ensina.

Os produtores de inteligência artificial, mais especificadamente sob os trabalhos desenvolvidos em que esta Autora presta consultoria em proteção de dados pessoais para empresas do ramo de inteligência artificial, teve o depoimento do CEO da empresa AIKNOW, que é possível

---

[126] TECHNOLOGY REVIEW. O Novo Gerador de Linguagem GPT-3. Disponível em: <https://www.technologyreview.com/2020/07/20/1005454/openai-machine-learning-language-generator-gpt-3-nlp/>, com acesso em 21/09/2020.

este tipo de situação onde o programador ensina e programa a máquina para determinada ação, mas que ela pode realizar outra diversa daquela planejada pelo programador, pois ela pode entender que a programação feita por ela própria atenderá melhor os requisitos do que a programação feita pelo seu programador.

Rogério Zero[127] afirma que mesmo havendo um programador que faça operações no sistema da inteligência artificial, o algoritmo pode aprender sozinho com aquilo que lhe fora ensinado e com base em todos os dados que lhe foram inseridos e informações transmitidas, ela pode desobedecer este comando.

Essa situação de *machine learning* acontece mesmo estando dentro de uma empresa em que há total controle e supervisão humana por detrás das máquinas. Perceba que é extremamente desafiador trabalhar com essa situação em que o programador se vê surpreendido numa situação como essa, quiçá a sua bagagem e expertises sejam extremamente necessárias e aí especialização em infraestrutura, desenvolvimento e segurança da informação para que este profissional da tecnologia possa contornar eventos dessa magnitude.

Tendo como ponto de partida que essas situações possam ocorrer no ambiente corporativo, e que há o direito ao avanço tecnológico, é de rigor que não haja imposição de medidas limitantes a inovação e a tecnologia. Em contrapartida, a supervisão humana é figura essencial, principalmente nos setores de tecnologia e de inteligência artificial.

Esta supervisão humana, deve ser feita por profissional normalmente graduado em bioinformática, engenharia de dados, tecnologia da informação, normalmente o controlador das operações e

---

[127] Depoimento colhido pela Mestranda em uma das aulas de Inteligência Artificial e Direito, onde atuou por todo o segundo semestre de 2019, sob a tutela dos Professores Ricardo Sayeg e Wiilis Guerra Santiago Filho, no mestrado da PUC/SP como ouvinte, e levou o seu cliente AIKNOW com o CEO Rogério Zero e o sócio-fundador Luís Cabañas para tratar do tema de Direito ao Desenvolvimento Tecnológico e a Proteção de Dados Pessoais.

supervisor do programador de algoritmos ou dos desenvolvedores de *softwares*, haja vista o campo de formação ter matérias como *frameworks*, metodologias de segurança, auditoria de sistemas e de privacidade de dados, de preferência, seria especialista e analista em segurança da informação, em governança de dados e em *cybersecurity*. Mas não basta apenas acumular títulos, esse profissional supervisor deverá ter experiências pragmáticas como a Lei Geral de Proteção de Dados pessoais ou com GDPR, pois desta forma, este profissional será completo para poder prestar relatórios técnicos e específicos ao advogado gerenciador do Programa de *Compliance* em proteção de dados pessoais.

Não obstante, o advogado gestor do Programa de *Compliance* deve possuir conhecimento teórico e prático para atuar com essas empresas em que se acredita estarem no topo da pirâmide de fiscalização da Autoridade Nacional de Proteção de Dados, em decorrência de sua força, de sua potência, e de sua alta escalabilidade.

É necessário quem é o advogado trabalhe juntamente com o profissional da área da segurança da informação para atuar principalmente e rapidamente neste tipo de demanda - *deep learning*, pois é uma situação que está fora do alcance das mãos do programador, e desta forma, deve estar bem perto dos olhos do supervisor (profissional da área de segurança da informação).

Essa é a razão para que o profissional advogado entre em ação, tomando como base uma primeira investigação buscando evidências de discriminação e preconceitos, em virtude de cruzamento de informações alimentadas pelo programador.

Sendo o advogado o profissional escolhido para ser o gestor do Programa de *Compliance*, representante da lei e defensor dos direitos humanos, deve extirpar combinações de questionamentos ao algoritmo ou buscas por informações do indivíduo que remontam à um possível ato discriminatório, e desta maneira corrigir o erro.

A constante auditoria deve ser presente no dia a dia destes profissionais para que se evite ao máximo o dano social, provocado pelo *deep learning*.

O profissional deve, sim, utilizar dessas novas ferramentas tecnológicas para facilitar a sua rotina e a comunicação entre os meios de execução do serviço que é prestado ao cliente e à sociedade, porém o profissional deve prever esse tipo de acontecimento, que é natural desses novos modelos de inteligência artificial, por isso, o profissional do futuro deve ser especializado nas matérias supraelencadas e estar no controle da situação para garantir a qualidade da prestação de serviços e nos casos em que a venda tem como processo final o próprio produto.

Esse profissional deve também além de saber utilizar dessas novas ferramentas tecnológicas, telas consigo na empresa, isso significa dizer que as empresas devem investir também não apenas em profissionais gabaritados, mas em aparelhos eletrônicos e digitais que permitam esse profissional controlar monitorar a qualidade do rastreio dos *logs* de acesso de todos os colaboradores, para que se tenha um contínuo aperfeiçoamento desses controles.

Desta forma o avanço tecnológico de mãos dadas com a segurança jurídica, permite contínua inovação; a tecnologia tem o direito de se expandir, mas com certas reservas e supervisão humana lhe auferindo limitações.

Nesta esteira, mesmo com toda essa proteção, a empresa incorrendo em qualquer situação discriminatória e preconceituosa, deve ter o cientista de dados à disposição para voltar ao laboratório e realizar novos testes para que não incorra em dano social.

Na realidade, esse profissional que normalmente tem conhecimento de matemática; física; mecânica; óptica geométrica, fluídica e comunicação visual; expressionismo; computação em elementos de *software*, telemática e *hardware*; redes de comunicação; matemática operacional; computação visual e gráfica; artes e humanidades; economia e produtividade. Uma educação contínua que o

engenheiro do futuro, conforme prevê João Antônio Zuffo[128] deve-se buscar como conhecimento básico, mas um conhecimento sólido para atuar na sociedade de dados.

Zuffo previu em 1997 sobre trabalhar em casa e as regras de intensa utilização de teleconferências, que é exatamente o que vem acontecendo, de maneira intensificada, após a ocorrência da pandemia provocada pelo novo Coronavírus, se essa previsão já era a visão de Zuffo, isso porque ele não previu uma pandemia, imagina a revolução que essa intensificação causou na sociedade, por isso, o termo “infoera” já está ultrapassado, e o melhor termo para ser utilizado nesta nova era é o dá “sociedade de dados” utilizado pelo filósofo Márcio Pugliesi.

O avanço tecnológico trouxe consigo confortabilidades ao ser humano, como diagnóstico médico auxiliado por sistema computadorizado de inteligência artificial, relatório comunicação de voz, telemonitoramento de pacientes, sintomas de pacientes já reconhecidos por sistemas eletrônicos, e isso fez com que os dados fossem atualizados a nível mundial, se tornando assim um *big data* para que a inteligência artificial pesquise com mais eficiência certas doenças, de acordo com os sintomas apresentados pelos pacientes.

João Antônio Zuffo[129] também já previa o que é a inteligência artificial poderia por meio de sensores acompanharam tratamento de imagens por instrumentos ligados por sensores ao paciente, a fim de acompanhá-lo interruptamente e diagnosticar com precisão simultaneamente, de maneira remota, dessa maneira tratar de forma mais precisa pelo acompanhamento em tempo real e por mais tempo realizado junto ao paciente, o que permitirá maior precisão do que quanto aos exames de imagens tradicionais.

---

[128] ZUFFO, João Antonio. **A Infoera: O Imenso Desafio do Futuro.** São Paulo: Editora Saber Ltda., 1997, p. 89-90.

[129] ZUFFO, João Antonio. **A Infoera: O Imenso Desafio do Futuro.** São Paulo: Editora Saber Ltda., 1997, p. 94.

Também já existe o auxílio pela inteligência artificial no campo do direito de sistemas especializados que possuem uma base de conhecimentos jurídicos auxiliando juízes em suas sentenças no Brasil, o que já ocorre no exterior. No Brasil, há o caso Watson, que atua em escritório de advocacia, do SINAPSES que ajuda a Advocacia geral da União, do VICTOR que auxiliar o Supremo Tribunal Federal[130], e do SÓCRATES 2.0, Utilizado pelo ministro João Otávio de Noronha Bing em termos de triagem, classificação processual, gestam de precedentes qualificados, leitura de peças processuais, comparação de textos, sugestão de controvérsias jurídicas, visualização de petição de recurso especial, realizados e monitorados pela inteligência artificial que está contribuindo com diversas soluções do trabalho no STJ, “E esse sistema está sendo ótimo para o STJ como afirma o ministro: “com o desenvolvimento de tecnologias que melhoram a triagem processual, buscamos racionalizar um imenso fluxo de processos que aportam diariamente da nossa corte de reduzir o volume de trabalho nos gabinetes dos ministros e elevar a qualidade das decisões, observando sempre os entendimentos definidos em matéria repetitiva. Além disso, queremos fortalecer a parceria entre o STJ e os tribunais de origem para dar mais efetividade ao instituto dos recursos especiais repetitivos”[131].

Mas o que importa efetivamente trazer é que a tecnologia está avançando e que ela necessariamente necessita do advogado para margear os seus limites e com isso, a LGPD foi perfeita, pois uniu a tecnologia e o jurídico em uma só legislação trazendo informações

---

[130] TECHNOLOGY REVIEW. O Novo Gerador de Linguagem GPT-3. Disponível em: <https://www.technologyreview.com/2020/07/20/1005454/openai-machine-learning-language-generator-gpt-3-nlp/>, com acesso em 21/09/2020.

[131] DETRAN. 2020. Detran vaza dados de CNH. Disponível em: http://www.detran;gob;br/Comunicacao/Noticias/23082020-Revolucao-tecnologica-e-desafios-da-pandemia-marcaram-gestao-do-ministro-Noronha-na-presidencia-do-aspx>, com acesso em 22/09/2020.

necessárias para que essas duas áreas diferentes caminhem juntas praticamente integralmente, de maneira que elas se completem.

Esses dois profissionais são extremamente capacitados para atuarem em meio a alguma situação desconfortável que ocorrer, sendo talvez, as maiores dificuldades de suas vidas, para se ampliar projetos e desenvolvimentos é necessária essa junção e o constante estudo científico em laboratórios, até que virtuais.

João Antônio Zuffo alerta para que haja enfatização da educação continuada de forma a se tornar a regra durante toda a vida profissional[132] do futuro que trabalhará com a tecnologia.

De certa forma, após toda essa transformação tecnológica e com o home-office, os profissionais não pretenderão limitar todo o conforto despejado em suas residências com auxílio dessas novas tecnologias, o que terá de fazer realmente com a segurança jurídica necessária e esperada pela sociedade, com a ajuda do operador de direito, pois esse trabalho deverá ser crescente.

O fato é que, aumentará a complexidade das tecnologias e da sua crescente evolução da microeletrônica, da nanotecnologia, dos computadores, da inteligência artificial, dos *softwares* e *hardwares* que serão projetados com mais velocidade, até pela própria era em que a sociedade vive e por todas as transformações e os acontecimentos, inclusive que na área da saúde, fizeram os indivíduos permanecerem em suas residências e utilizarem com mais frequência os aparelhos eletrônicos e digitais em decorrência da pandemia causada pela COVID-19 (SARS-CoV-2).

## 3.2 Mudando a Cultura da Empresa

Desde o dia 14 de agosto de 2018, as empresas necessitaram criar uma estratégia para se adequar à Lei Geral de Proteção de Dados Pessoais e, então, oferecerem um cenário diferente ao que tudo

[132] ZUFFO, João Antonio. **A Infoera: O Imenso Desafio do Futuro.** São Paulo: Editora Saber Ltda., 1997, p. 91.

ultrapassado um dia foi. Mas essa adequação não pode ser mais um atendimento como outras legislações; desta vez, é diferente; o Brasil tem uma Lei que protege especificamente os dados pessoais dos indivíduos e é com todo o cenário exposto sobre a proteção dos direitos fundamentais que esta Autora busca trazer ao conhecimento público, que as empresas necessitam conhecer um *compliance* em proteção de dados fundado na filosofia do Direito, como forma de conscientizar as empresas a não incorrer em discriminação e preconceitos, pois essas duas palavras carregam dor, violência e muito sangue.

As empresas precisam saber que o Programa de *Compliance* em LGPD é muito maior do que se adequar a legislação, ele ultrapassa a proteção dos direitos fundamentais, porque não visa apenas proteger os dados pessoais dos titulares, além de obstar o dano social, pelo próprio fundamento de sua prevenção. O “Programa de Compliance LGPD do Brasil” visa mostrar as empresas o que é um simples descumprimento legal pode afetar não só à uma pessoa, mas à uma sociedade como um todo, haja vista a infoera ter ultrapassado essa denominação e hoje ser chamada de sociedade de dados − aquela que carrega na raiz os instantâneos aprimoramentos de novas tecnologias e aperfeiçoamento da inteligência artificial. Isso significa dizer que, uma alta escala de produção do tratamento de dados pessoais, sem cuidados prévios, prejudicará à humanidade, à sua paz social e ao bem-estar social, ocasionando derramamento de sangue inocente, como foi no passado.

Talvez o que ocorreu no passado não se replique da maneira como foi, mas acredita-se que o suicídio em massa seja um novo derramamento de sangue, pois a nova sociedade de dados, e sobretudo após a passagem do desastre psicológico nas pessoas causado pelo novo Coronavírus, aliado ao uso de dados pessoais indiscriminados por *cyber* criminosos, implique diretamente neste assunto.

Há uma série de acontecimentos que podem ocorrer com o *hackeamento* de dados pessoais por *cyber* criminosos ou mesmo vazamento dos dados e informações no âmbito eletrônico e digital, desde

a utilização de dados pessoais para compras via internet, para cadastramento em programas de filmes, para a inclusão em algum clube de jogo de futebol, para uma assinatura de internet, por se passar pelo indivíduo com intuito de se beneficiar financeiramente, pedindo dinheiro aos amigos e familiares próximos da pessoa a qual teve a conta *hackeada*, dentre outros. São inúmeros os acontecimentos e que dependendo do momento em que a vítima se encontrar, pode sim, influenciar de tal maneira na vida dela que lhe cause doenças terríveis como a síndrome do pânico, crise de ansiedade, taquicardia, arritmias cardíacas, e até uma depressão fatal.

A depressão foi elencada como a doença mais incapacitante no ano de 2020 no mundo inteiro[133], e é considerada líder no *ranking* das doenças, considerando o tempo vivido de incapacitação ao longo da vida com 11,9%[134]. Essa expectativa da Organização Mundial da Saúde disparou em razão da imprevisibilidade da circulação do vírus Sars-CoV-2 (novo Coronavírus), vírus tão poderoso que foi capaz de infectar, de tabela, até pessoas que não foram infectadas pelo próprio vírus, mas a influência social, pelo distanciamento social que ele rapidamente promoveu entre as pessoas.

Então o aumento do trabalho *home-office* com as responsabilidades de área que cada indivíduo carrega em suas próprias vidas trouxe um efeito devastador provocado pela profunda tristeza do indivíduo se ver longe de outros que o deixavam feliz. A ausência da felicidade tornou a tristeza frequente e intensa durante o período de quarentena entre os afetados pela doença e entre os que por força da pandemia tiveram que manter certo distanciamento social.

---

[133] G1. 2020. Disponível em: <https://g1.globo.com/sp/presidente-prudente-regiao/blog/psicoblog/post/2020/01/12/depressao-a-doenca-mais-incapacitante-de-2020.ghtml>, com acesso em 23/09/2020.

[134] Idem.

O fato de mencionar essa terrível doença e sobre a sua devastação invisível, aliada a dados pessoais nas mãos de empresas que não tem um mínimo conhecimento para tratar dos dados pessoais, ou ainda que tenha conhecimento, não saibam exatamente o porquê a legislação de 2018 chegou, devem conhecer o histórico da proteção à privacidade do indivíduo. Porque com todos esses acontecimentos, até o general Heleno, chefe do gabinete de segurança institucional da Presidência da República acabou por ter um grande descuido com os seus dados pessoais e a ironia daquela frase antiga de que “casa de ferreiro espeto de pau”, se encaixou na vida do general Augusto Heleno, que se tornou rapidamente, perante as redes sociais, motivo de piada.

O general Augusto Heleno que é responsável pela inteligência do governo foi infectado pelo novo Coronavírus e, como ele, estava na linha de frente ao combate dessa doença para ajudar o governo, quando foi realizar novo teste e esse teste apontou ser negativo para o novo Coronavírus (COVID-19), general Heleno, feliz, publicou uma foto do resultado de seu exame onde constavam dados pessoais como seu nome completo, o seu RG, e o seu CPF.

Este acontecimento se deu em 31 de março de 2020, sob estado de euforia, justamente porque no dia 17 do mesmo mês, ele havia testado positivo para doença e postou a foto desse resultado negativo agradecendo o apoio das pessoas, à Deus, às orações que fizeram, e aos seus amigos.[135]

Figura 1 : Alusão à invasão de privacidade do General Heleno

[135] CORREIO BRASILIENSE. 2020. General Heleno e o Vazamento de Dados. Disponível em: <https://www.correiobraziliense.com.br/app/noticia/politica/2020/03/31/interna_politica,841485/ao-postar-exame-general-heleno-esquece-de-apagar-dados-pessoais.shtml>, com acesso em 23/09/2020.


136

Fonte: Correio Brasiliense (2020).

Acontece que, rapidamente, as curtidas foram aumentando em seu perfil do Twitter até que um *cyber* criminoso decidisse por se utilizar dos dados pessoais do general Heleno para assinar um perfil no Globoplay, uma filiação partidária do Psol, realizar a consulta de seu nome nos dados restritivos de proteção ao crédito, de escrevê-lo como mesário, dentre outros[137].

O que se espera de um chefe da segurança e da inteligência da presidência da República é que no mínimo esta pessoa tenha conhecimento sobre o quão são poderosos os dados pessoais e a relação que a quantidade de dados pessoais somadas têm para traçar um perfil

[137] Jornal O Estadão. Vazamento de dados General Heleno. Disponível em: <https://politica.estadao.com.br/noticias/geral,apos-piadas-na-internet-heleno-borra-dados-pessoais-de-resultado-de-coronavirus,70003255441>. Acesso em 22/06/2021.

do indivíduo e para devastá-lo, já que como falado anteriormente neste trabalho, o dano social causado pelo manuseio errado desses dados pessoais pode gerar, pois não há como saber a quantidade exata de pessoas que tiveram acesso a esse documento e a quantidade de pessoas que salvou esses dados e que poderão utilizá-los deles em qualquer época para fins inimagináveis, ficando assim, a punição um objeto sancionatório quase que ineficaz perto do que o uso indiscriminado da tecnologia pode causar.

Extensão do dano social mais grave do que esse seria então morte de pessoas em massa, já que, assim como a inteligência artificial tem alta escalabilidade em um curto período, a reprodução de dados pessoais lançados no âmbito da internet tem o mesmo efeito e esse efeito se torna sem fronteiras, pois não há limite para territorialidade, assim como não há limite para predizer ações humanas das quais armazenaram os dados pessoais de alguém que foi vitimado.

O que se busca trazer neste trabalho é que o advogado que irá comandar a operação de *compliance* em proteção de dados pessoais nas empresas informe e conscientize sobre o plano de fundo da LGPD, que não está limitado apenas a GDPR, mas à uma história que deve ser respeitada e então ter como missão de elevar os padrões de segurança, dando interpretação ampliada para a Lei Geral de Proteção de Dados Pessoais.

A GDPR traz os princípios de defesa embasada nos direitos humanos, ou seja, os dados pessoais são considerados como direitos inerentes a personalidade da pessoa humana, observando a inviolabilidade da vida privada.

Não é que o advogado deterá qualquer atitude preconceituosa ou discriminatória que ocorrer no âmbito profissional nas empresas, mas esse processo de adequação é essencial porque ele ocorre no campo invisível - prevenção, que de certa maneira ocorrendo algum fato ou ato que vá contra a legislação de proteção de dados pessoais brasileira, existe toda uma estratégia da qual demonstrará o que a empresa procurou se reservar de mecanismos e procedimentos internos capazes

de minimizar o dano, voltados à um tratamento seguro e adequado[138], justamente porque, com a adesão, a empresa demonstra boa-fé e com isso, o grau da infração que vier a incorrer será bem menor do que se ela não iniciar o "Programa de *compliance* LGPD do Brasil" em proteção de dados pessoais, ou ainda, se tiver iniciado e até finalizado um projeto, mas que ele não seja um programa supervisionado por especialistas, então por mais que haja boa-fé, o grau do dano será maior, pois a empresa então, não adotou medidas de segurança necessárias, como por exemplo, as boas práticas e da política de governança, não havia a previsão efetiva de medidas corretivas sobre determinado evento porque a empresa não reservou o capital condizente com a sua situação econômica que lhe permitisse contratar uma equipe que, de fato, pudesse atender e adequar a empresa.

Acontece que, com o objetivo de economizar, mesmo que a empresa tenha um capital reservado para investimento com *Business Inteligence*, ela não está disposta a investir na medida em que uma equipe preparada e especializada poderá dar todo o suporte, treinamento inserção do programa de *compliance* em proteção de dados pessoais. Quando a empresa busca essa economia e contrata um profissional, que pode ser até especialista, mas que, não tenha uma equipe preparada para atender o porte daquela empresa contratante, não haverá correspondência entre a prestação de serviço e o serviço prestado, não há qualquer concordância nessa parte, pois todo trabalho tem seu valor e toda equipe tem o seu custo.

Outra forma de engano das empresas, que é gravemente condenada pela LGPD é não adotar mecanismos de proteção de dados pessoais e do tratamento deles que atendam a nova sociedade de dados, ou pelo menos, a infoera; que tende a trocar equipamentos eletrônicos digitais por mais modernos, está com processamentos mais rápido, com armazenamento mais seguro (*cloud*) que já atenda padrões do Regulamento Europeu 679/ 2016 (GDPR), que tenha camadas de segurança desde o mobile até a *cloud*.

---

[138] Art. 52, §1º, da Lei 13.709/2018 (VADEMECUM SARAIVA, 2020).

Por que a LGPD se importa com o faturamento total da empresa ou do grupo de empresas? o capital deve ser reservado na proporção do seu recebimento, isso significa dizer que, a Autoridade Nacional de Proteção de Dados, aquela que vai fiscalizar as empresas e aplicar as medidas corretivas face às sanções e punições levará em conta esse valor[139], até mesmo para fazer a dosimetria da multa.

Durante o estudo em campo desta Autora, percebeu-se a falta de entendimento sobre o tema versus a urgência necessidade de conscientização da lei, mas pelo fato de terem a intenção e vontade de contratar serviços avulsos, para satisfazer um cumprimento legal, que no pensamento deles, a LGPD fica adstrita à política de privacidade e termos e condições de uso.

A adequação a Lei Geral de Proteção de Dados Pessoais não é apenas um projeto onde o profissional advogado vem com a sua equipe e atende determinadas horas à empresa, regularizando apenas o estatuto, os regulamentos e as suas políticas, e vai embora, finalizando o projeto como se fosse uma instalação de serviços tecnológicos que tem início, meio e fim para a entrega. Para uma empresa estar devidamente em *compliance* com a LGPD, ela necessita de uma assistência permanente e intercorrente, de assessoria jurídica com equipe multidisciplinar e multiprofissional, para iniciar o "Programa de C*ompliance* LGPD do Brasil" e tornar a empresa apta para atender com transparência o seu cliente, colaborador, prestador de serviço e fornecedor de serviço, então, assim passarão a administrar o projeto realizado, do qual terá contínuas atualizações, supervisão, treinamentos, administração de contingenciamento, defesas do

---

[139] **Art. 52**. *Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: [...]*

*II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração.* [...]

contencioso, manobras conciliatórias a fim de minimizar ainda mais os danos sofridos pela empresa.

Aqui, esta Autora propõe o programa completo em LGPD, do qual iniciará um atendimento à empresa sendo que o líder da operação é um advogado especializado em proteção de dados pessoais, em direito eletrônico ou direito digital, mas que tenha a base da filosofia do Direito. O advogado líder desta operação deve necessariamente ter uma base de formação em filosofia do direito para transmitir ética à empresa, para não acobertar atos discriminatórios ou preconceituosos e se existir, eliminá-los, pois caso contrário, o profissional que vê este tipo de situação e não toma providências imediatas, é como se fosse um agente transgressor da norma, pois poderia ter feito algo e nada o fez.

Por isso, a reiteração desta Autora em que a base seja no campo da filosofia do Direito - campo em que se pode entender tudo o que a sociedade precisa, ou pelo menos, buscar entender para que então essa busca o leve em algum lugar diferente do que normalmente outros profissionais estejam habituados a fazer. O raciocínio a percepção e a cognição são institutos indissolúveis que deverão seguir com um profissional advogado que liderará este processo.

## *3.3* “Protocolo LGPD-BR”: Como Preparar o Ambiente Corporativo para a Recepção da LGPD?

O advogado deve em seu escritório de advocacia, ter uma equipe multiprofissional no mínimo formada em direito, em tecnologia da informação, com todas as especializações já mencionadas no subtítulo anterior. Nesta equipe pode ter bacharel em Direito, assistentes administrativos, assistentes jurídicos, advogados especialistas em proteção de dados pessoais, advogados conformação de mestrado ou doutorado em filosofia do direito, advogado especialista, de preferência na área de atuação específica do segmento da qual o seu cliente necessita da prestação de serviços.

O advogado ao visitar a empresa, deve necessariamente, conhecer muito bem o ramo de atuação da empresa da qual vai prestar serviços, pois o "Programa de *Compliance* LGPD do Brasil" deverá atender os funcionários desta empresa, os seus colaboradores, os seus prestadores de serviço, os seus fornecedores, e os seus clientes, de uma maneira totalitária e uniforme. Não pode o programa atender apenas só clientes ou só prestadores de serviços ou só colaboradores; o programa deve atender à todos, caso contrário, aquele modelo de projeto não será eficaz e até me parece que muito amador, colocando inclusive, em risco iminente à empresa da qual prestará esse serviço, que se sentirá seguro por ter serviços vendidos separadamente à um preço menor, é claro, a mais que não lhe fornecerá segurança jurídica quanto a proteção dos dados pessoais tratados por ela.

Bem, o "Programa de *Compliance* LGPD do Brasil" deve seguir o "Protocolo LGPD-BR"[140], que compreende identificar o cenário atual da empresa (assessment), qual o advogado prestará serviços, incluindo os seus processos internos, a sua tecnologia contratada, a sua forma de governança entre os funcionários, a confirmação de políticas existentes nesta empresa, entender o funcionamento de normas e regras internas (regimento interno), avaliando de forma crítica todo esse cenário inicial em comparação aos ditames da Lei Geral de Proteção de Dados Pessoais.

Na sequência, o advogado precisará avaliar o inventário de dados pessoais da empresa, catalogando quais são os dados pessoais trafegados no sistema e qual é esse sistema utilizado, se e se ele está incompleto para atender essa demanda, inclusive neste ponto, o advogado deverá auditar o volume de dados pessoais fazendo uma

[140] O "Protocolo LGPD-BR" foi criado por esta Autora no desempenho de função na Advocacia Baccari como Assessora Jurídica no "Programa de *Compliance* LGPD do Brasil" às empresas que aderiram a implementação da adequação à Lei 13.709/2018. Este protocolo segue fases pré-determinadas na "Rota de *Compliance*" que foram traçadas obedecendo critérios de proteção jurídica, tecnológica e de processos. Todas as denominações utilizadas no "Programa de *Compliance* LGPD do Brasil" são de autoria própria e estão disponíveis em seu domínio www.LGPDdoBrasil.com.br.

menção crítica sobre a necessidade do tratamento de todos os dados pessoais envolvidos, para que, ao final fiquem apenas dados essenciais para o tratamento realizado pela empresa.

Após isso, o advogado deverá identificar qual é o controle tecnológico que a empresa tem com os dados pessoais e a forma como eles são tratados, analisando a infraestrutura do suporte técnico, como seu armazenamento (*cloud* ou data center), identificar a territorialidade onde eles estão armazenados, inclusive se há transferência Internacional desses dados pessoais, ou se não houver identificar o fluxo dos dados pessoais, bem como o seu ciclo de vida. Nesta etapa, é necessário analisar se o titular do dado deu consentimento para que a empresa faça este tratamento, não sendo este o caso, a empresa então, deve analisar as bases legais na LGPD que possibilite o tratamento sem o *opt-in*.

Realizar uma auditoria nos documentos internos da empresa, como regulamento interno o contrato de trabalho dos funcionários, dos prestadores de serviço, dos colaboradores, e o contrato de prestação de serviços com os clientes, bem como as políticas de governança e de privacidade os termos de uso e de consentimento, os termos de sigilo é confidencialidade, os NDA em geral, e atualizá-los.

O advogado deve sistematizar todos os setores da empresa fazendo um mapeamento por onde os dados passam e quais os profissionais têm acesso a eles, inclusive, já alterando o seu processo e o seu funcionamento, deixando passar por setores obrigatórios e treinar essas pessoas, principalmente as que tiverem acesso a informações pessoais e dados sensíveis dos quais merecem um amparo sigiloso, com graus, inclusive, de segredo.

Em ato contínuo, entra em campo o profissional da área de tecnologia da informação e segurança (*personal cybersecurity*), este que irá identificar as vulnerabilidades do sistema, realizando testes (*Pentest*) que apontaram a violação ou algum facilitador de meio para o qual o *cyber* criminoso, ou um *cracker*, possa invadir o sistema operacional da empresa, vazar dados pessoais ou, ainda, serem encontrados erros

sistêmicos que permitam a falha e a visualização de dados que eram para ficar fechados e de acesso somente para certo grupo de determinado setor da empresa.

O advogado deve acompanhar toda essa avaliação e relatório sobre os dados pessoais não estruturados em pastas de arquivos, inclusive físicos e eletrônicos, que também é realizada pelo profissional da segurança da informação, o teste é conhecido como Scan[141], orientando a empresa quanto a esse armazenamento, apontando ainda soluções para tanto, caso haja.

Após a emissão dos relatórios, o profissional da tecnologia da informação e segurança deve apontar as vulnerabilidades do sistema e orientar quanto a eventuais lacunas e falhas em que merecem ser corrigidas por meio de uma complementação de produtos, em *softwares*, ou ainda da substituição de *softwares*, ou ampliação desses meios eletrônicos que lhe confira maior segurança e proteção no tratamento de dados pessoais.

Com este cenário o advogado já tem base de conhecimento o suficiente para, então, iniciar a sua estratégia nesta empresa e descrever o modelo atual, e o modelo do Programa de Compliance LGPD, dando o seu parecer sobre o que auditou e analisou.

A partir daí, o advogado vai começar então a atualizar, a criar, ou editar as normas e os regulamentos internos da empresa de acordo com o apontamento feito em seu parecer, fundamentando sempre a não-discriminação e o não-preconceito, garantindo que todos os direitos trazidos na Lei Geral de Proteção de Dados Pessoais foram cumpridos por essa empresa, a fim de torná-la adequada a recepção da LGPD, mitigando os riscos de Infrações.

Os incidentes que forem captados e os eventos ocorridos devem, de fato, obedecer ao manual de boas práticas e que este seja

---

[141] *Software* que realiza pesquisas de dados pessoais e sensíveis em uma máquina ou celular a fim de verificar pontos de vulnerabilidades sobre possível infração à LGPD. Esta informação foi obtida com os trabalhos em campo realizados na Advocacia Baccari.

efetivo, devendo o advogado treinar toda a equipe para receber a princípio, o *workshop* sobre a Lei Geral de Proteção de Dados Pessoais, e assim identificar os grupos de cada setor que serão responsáveis por cada operação e treiná-los de maneira individualizada.

É desejável que esse escritório de advocacia tenha uma equipe de conciliadores, árbitros e mediadores que realizem esse tipo de acordo amigável em seu próprio escritório, tudo para a composição em redução de despesas e gastos da empresa, o que é inclusive, totalmente recomendável é um direito contido na LGPD. Por meio de consultoria estratégica, oferece amparo técnico com mediadores capacitados e assessoria jurídica para solucionar conflitos sem a intervenção do Estado.

As plataformas dos sítios eletrônicos da empresa deverão ser auditadas para que todo o seu funcionamento e regramento estejam de acordo com a legislação.

Analisando o risco que a empresa tem inerente à sua atividade de prestação de serviço, como é o caso de empresas que estão no topo da pirâmide para visita da autoridade nacional de proteção de dados pessoais o que são empresas de tecnologia, que desenvolvam ou licenciem *softwares*, que produzem ou prestem serviços de inteligência artificial e que tratem com dados sensíveis, como por exemplo, é o caso das igrejas, hospitais, clínicas médicas e inclusive, o Poder Público se enquadra em qualquer destas categorias. Identificando a categoria do seu cliente, e avaliando o risco; o advogado deve indicar seguro de responsabilidade no caso das informações no tratamento de dados pessoais.

O advogado deve analisar a equipe de segurança da informação e verificar se há entre alguém que componha o setor de controle, indicando os profissionais que serão controlador, o operador, e o encarregado dessas operações, inclusive indicando e criando meios de comunicação dessas pessoas entre o titular de dados e a autoridade nacional de proteção de dados, sendo eles eletrônicos e físicos, com a publicação da pessoa responsável que ficará encarregada de tomar

frente deste programa nas comunicações entre os sujeitos da Lei, que é o tal do encarregado, conhecido internacionalmente como “DPO” – *Data Protecion Officer*[142].

Como se trata de um programa, deve haver pesquisas de satisfação que verifiquem e analisem a resposta do programa perante as pessoas que estão dentro da empresa, os seus clientes e a sociedade de maneira geral, pois é a sociedade que precisa saber que o seu cliente, ou seja, essa empresa, está se atualizando e tomando providências para atender à proteção de dados pessoais adequadas ao indivíduo, ademais podendo ser até beneficiada como um jogo de *marketing*.

Certamente que a empresa necessitará desse escritório de advocacia para dar amparo em resposta a possíveis notificações que necessitarão responder à Autoridade Nacional de Proteção de Dados, inclusive com prazo para isso, ressaltando-se que a lei, apesar de tratar um prazo razoável, 72 horas[143], tem a intenção de ter esse regulamento como plano de fundo, devendo então ter o espírito dela.

Além das defesas administrativas que irão surgir, é de se esperar que litígio e que demandas judiciais seja um futuro do contingenciamento das empresas, em decorrência do mau tratamento de

---

[142] **Artigo 14 do Regulamento Europeu 679**. *Informações a facultar quando os dados pessoais não são recolhidos junto do titular.*

*Quando os dados pessoais não forem recolhidos junto do titular, o responsável pelo tratamento fornece-lhe as seguintes informações: a) A identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante; b) Os contactos do encarregado da proteção de dados, se for caso disso*. [...] [grifo nosso]

[143] **Artigo 33 do Regulamento Europeu 679**. *Notificação de uma violação de dados pessoais à autoridade de controlo 1. Em caso de violação de dados pessoais, o responsável pelo tratamento notifica desse facto a autoridade de controlo competente nos termos do artigo 55.o, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares. Se a notificação à autoridade de controlo não for transmitida no prazo de 72 horas, é acompanhada dos motivos do atraso*. [grifo nosso]

dados pessoais e de diversas reclamações, por isso, o escritório de advocacia é indispensável, pois é ato exclusivo de advogado.

Veja-se que o acompanhamento deste programa deve ser contínuo e que haja constantes campanhas sobre a conscientização da Lei Geral de Proteção de Dados Pessoais e suas intensas melhorias.

É necessário apontar o que o serviço de assessoria jurídica na sociedade de dados deverá ter um apoio de um advogado que tenha esse perfil, pois é a oportunidade que a empresa tem de mudar a cultura interna e o respeito com as pessoas. Apesar de ser um grande projeto, o profissional deve tratá-lo como programa, pois só assim ele terá eficácia plena e maior segurança para a empresa, que por consequência, terá menos risco porque agiu corretamente como esperado pelo legislador brasileiro.

Deve-se obstar o abuso de direito pelas empresas, pois a empresa tem um poder e como já vimos poder e controle precisam estar na mão de pessoas capacitadas e treinadas para tanto.

O relatório de impacto à proteção de dados pessoais a ser enviado à Autoridade Nacional de Proteção de Dados apenas quando o programa estiver implementado na empresa, claro, após ter informado ao cliente do cliente que os dados estão cadastrados e que ele tem o direito de acessar gratuitamente as informações sobre ele existentes no banco de dados; irrestritamente ter acesso ao seu histórico; impugnar qualquer informação sobre ele erroneamente anotada em banco de dados; conhecer os principais elementos e critérios considerados para a análise de risco, resguardado o segredo empresarial; ser informado previamente sobre o armazenamento; a identidade do gestor do banco de dados, o objetivo do tratamento dos dados pessoais e os destinatários dos dados, em caso de compartilhamento (art. 5º da LGPD )[144].

---

[144] SUPERIOR TRIBUNAL DE JUSTIÇA, 2020. Recurso Especial n. 1.457.199 - RS. Disponível em: <https://bdjur.stj.jus.br/jspui/bitstream/2011/114173/REsp1457199.pdf>, com acesso 23/09/2020.

A empresa deve garantir o mínimo necessário para proteger os dados, não importa o porte, todas devem se adequar. Ela deve garantir com clareza aos titulares a consulta gratuita e facilitada sobre a forma e a duração do tratamento de dados dos titulares, e que eles podem ser atualizados, a qualquer momento, nos meios físicos e eletrônicos.

Não obstante de tudo, o que a empresa deve fazer para se tornar *compliance* em LGPD, deve ter um espírito de responsabilidade social em manter acesa a chama dos direitos fundamentais que garantam a proteção e a inviolabilidade da vida privada do indivíduo, sobretudo, ter cuidados excessivos com o tratamento de dados pessoais que podem ser alguma fonte de discriminação e preconceitos que não podem sobreviver. Esta é a missão dos advogados que se têm vontade de trabalhar com esse tema no Brasil.

O “Protocolo LGPD-BR” é firmado em 04 pilares básicos, além da consultoria jurídica e em cibersegurança: auditoria, plano de estratégia, execução e administração do “Programa de *Compliance* LGPD do Brasil”.

Seguir o Protocolo LGPD-BR significa passar por 24 (vinte e quatro) fases de adequação e seguir a rota de *compliance* traçada por esta Autora, desta forma, evitando saltos[145], para que haja uma implementação adequada.

Na auditoria é feita uma análise da apresentação da empresa que será vital para enxergar a atual situação de não-adequação à Lei 13.709/2018; com isso será possível traçar um plano de estratégia e customizar o “Protocolo LGPD-BR” com as falhas e vulnerabilidades encontradas; já adentrando na execução em si; e por último administrar e atualizar as boas práticas implementadas com estratégia de auditoria contínua.

---

[145] O Salto significa pular a etapa sem que ela tenha sido iniciada e/ou concluída.

Cada fase deve ser rigorosamente seguida, sendo extremamente vedado o salto[146] de fase[147], pois prejudicará a adequação da empresa.

O Fluxo do "Programa de *Compliance* LGPD do Brasil" possui a seguinte disposição:

- Palestra inicial
- Identificação do cenário
- Verificação de Vulnerabilidades Sistêmicas (*Pentest*)
- Criação e Inauguração do Setor de Controle
- Análise do Perfil do DPO
- Criação e Inauguração do Canal do Titular de Dados
- Mapeamento do Fluxo dos Dados (Entrevistas e *Scan*)
- Análise de Processos e Tecnologias
- Avaliação do Modelo Atual da Empresa
- Atualização ou Confecção dos Termos e Políticas de Privacidade Externa (Sites)
- Atualização ou Confecções de Contratos, Políticas Internas, Código de Ética dos Algoritmos e Regulamento Interno, Acordos Comerciais e Termo de Sigilo e Confidencialidade (NDA)
- Treinamentos com a Equipe
- Realização de Campanhas de Conscientização
- Oferecimento de Suporte no Relacionamento com Clientes e com a Autoridade Nacional de Proteção de Dados (ANPD)
- Início da Pesquisa de Satisfação.

---

[146] As consequências são graves, pois a Advocacia Baccari não terá uma avaliação técnica definida sobre o cenário atual da empresa, desta forma, não haverá base intelectual de entendimentos de processos e tecnologia o suficiente para que o trabalho seja entregue de maneira responsável e segura.

[147] As fases foram criadas de acordo com a metodologia da Autora durante os estudos, desenvolvimento e escrita deste trabalho.

### 3.3.1 Palestra Inicial

A palestra é uma fase de suma importância para o “Programa de Compliance LGPD do Brasil” e deve ser realizada por especialista em LGPD.

A empresa deverá convidar os principais gestores dos departamentos de RH, Financeiro/administrativo, Tecnologia da Informação, Juridico e sócios com o objetivo de levar informação sobre a Responsabilidade Social das Empresas na Proteção de Dados Pessoais, com a oportunidade de os profissionais fazerem perguntas e terem respostas e consultoria imediata.

### 3.3.2 Identificação do cenário

Esta fase consiste em iniciar a identificação do cenário em que a empresa está e deve ser acompanhada pelo questionário de adequação para que haja auditoria em todos os departamentos da empresa. Desta forma, é possível criar o caminho que os dados pessoais percorrem na empresa.

### 3.3.3 Verificação de Vulnerabilidades Sistêmicas (Pentest)

É o processo de implementação que analisa a Empresa de forma integral: processos – tecnologia - jurídico, correspondente a fase “Verificação de Vulnerabilidades Sistêmicas", que deve ser realizada pelo Profissional Personal CyberSecurity responsável pela execução e elaboração de relatório técnico.

Deve ser enviado um NDA (termo de sigilo e confidencialidade) com a autorização de que a Empresa consente a execução dos serviços estilo do *pentest black-box, grey-box* ou *white-box*.

E orientado que se execute o *pentest*, ao menos uma vez ao ano, quando a empresa for de pequeno porte, e as demais, deverão ser analisadas de acordo com a sua operação e seguimento.

### 3.3.4 Criação e Inauguração do Setor de Controle

O Setor de Controle é o departamento que supervisionará as atividades dos colaboradores da empresa no que diz respeito ao cumprimento da Política de Privacidade Externa e Interna; atuará na qualidade e na prevenção de eventos e incidentes promovendo a boa prática diariamente entre os setores da empresa; auxiliará o DPO nas questões do cadastro pessoal dos titulares.

### 3.3.5 Análise do Perfil do DPO

O DPO (*Data Protection Officer*) – mais conhecido no Brasil como “encarregado”, é o profissional que vai se comunicar com a Autoridade Nacional de Proteção de Dados (ANPD), com o titular dos dados (cliente, cliente do seu cliente, colaboradores ou fornecedores), com o seu cliente, com o Poder Judiciário ou outra autoridade competente de compliance, e com o Escritório de Advocacia que fará o *compliance*.

Esse profissional pode ser qualquer pessoa que tenha habilidade de comunicação, inclusive de boa escrita e leitura para lidar com problemas administrativos levados às pessoas supracitadas, que conheça muito bem os processos e tecnologias da Empresa e que esteja disponível para atuar quando a empresa sofrer algum tipo de vazamento de dados, ataque cibercrime, notificação da Autoridade Nacional Proteção de Dados, explicações de titulares, e atuação como testemunha nos casos em que for judicializada a situação. Além de conhecer muito bem a Política de Privacidade, de Governança, Termos de Uso, Consentimento e o Código de Ética. Deve ser alguém de confiança. Normalmente, as empresas escolhem o Gerente da Tecnologia da Informação.

### 3.3.6 Criação e Inauguração do Canal do Titular de Dados

Após as pessoas escolhidas pela empresa, deve-se então, criar e inaugurar o setor que estará em contato com o titular dos dados quando

houver qualquer solicitação por parte dele, em qualquer de seus direitos[148] carreados na LGPD.

### 3.3.7 Mapeamento do Fluxo dos Dados (Entrevistas e *Scan*)

O mapeamento do fluxo de dados pessoais é arquitetado, conforme o que foi informado pela empresa, por isso, a extrema necessidade de noticiar os processos verdadeiros que são executados por ela, por mais errados que sejam. Para isso o escritório de advocacia atua, identificando os procedimentos internos que geram risco a proteção de dados pessoais.

Desta forma, norteia sobre os riscos envolvidos e orienta sobre as mudanças necessárias, para que a empresa faça tomada de decisões juntamente com os seus gestores, e ao final, contribua para o seu protocolo de adequação.

As estratégias que melhores avaliam essa questão para apurar o inventário de dados por cada setor operado por cada chefia ou gestão

---

[148] **Art. 18**. *O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:*

*I - confirmação da existência de tratamento;*

*II - acesso aos dados;*

*III - correção de dados incompletos, inexatos ou desatualizados;*

*IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;*

*V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019) Vigência*

*VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;*

*VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;*

*VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;*

*IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.*

daquela operação são as entrevistas realizadas com os líderes de cada departamento da empresa e com a rodagem do *Scan*.

Essa fase consiste na ampliação as análises sistêmicas, o *report* de *hardware* e *software*; verificações de modificações de instalação e *discovery* de rede; inventário de dados sensíveis; consultoria via acesso remoto; verificação de *software* desatualizado, e *scan* por palavra-chave; neste período de rodagem.

### 3.3.8 Análise de Processos e Tecnologias

Após as fases supracitadas, é possível analisar com afinco os processos e tecnologias utilizadas pela empresa, então para isso, deve-se realizar entrevistas com a liderança do Departamento de Tecnologia da Informação/ Desenvolvimento de *Software*/ Algoritmos, do Recursos Humanos/ Administrativo/ Financeiro, ou, na falta destes, com o próprio CEO da empresa.

São apuradas informações complementares descritas no Questionário de Adequação[149], por isso, o profissional deve, necessariamente, conhecer os processos internos como a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação dos dados pessoais e o controle, modificação, comunicação, transferência, difusão, e extração que a empresa tem sobre eles, tanto com colaboradores, clientes, fornecedores e parceiros.

---

[149] Questionário de Adequação é um documento que contém várias perguntas relacionadas à LGPD formuladas pelo Escritório de Advocacia que realiza a implementação do "Programa de Compliance LGPD do Brasil". Vide artigo escrito pela Autora em sua coluna de Inteligência Artificial e LGPD no Diário Popular de São Paulo disponível em: <https://www.diariopopulardesp.com.br/colunistas/post/o-tal-do-questionario-de-adequacao/566/>. Acesso 23/06/2021.

### 3.3.9 Avaliação do Modelo Atual da Empresa

Até esta fase cumprida, o Advogado já tem subsídios para avaliar o grau de *compliance* que a empresa apresenta em relação à Lei 13.709/2018 e dar o seu parecer.

O parecer deve conter especificadamente todos os pontos da Avaliação de Processos e Gerenciamento de Incidentes e Violações, inclusive com Recomendações e GAPS (falhas operacionais) visualizadas pelo Advogado Especialista e pelo *Personal CiberSecurity*[150] em um Relatório Técnico em Processos e Tecnologias aplicados.

### 3.3.10 Atualização ou Confecção dos Termos e Políticas de Privacidade Externa (Sites)

A Política de Privacidade e os Termos e Condições de Uso[151] são documentos confeccionados pelo Advogado para que a empresa tenha disponível em seus sítios eletrônicos e obedecer a alguns pontos

---

[150] Profissional especializado em Segurança da Informação e crimes cibernéticos.

[151] Deve conter informações de [...] *usuários, layout, senha, site, funcionalidades disponíveis na plataforma, condições de acesso e restrições de funcionalidade, modalidades de cadastro e acesso, obrigações da organização, obrigações do usuário, obrigações de segurança da informação pertinentes às partes, casos de limitação de responsabilidade e isenção, direitos autorais e propriedade intelectual, multas e penalidades, denúncia e rescisão, formas de comunicação entre as partes, questões referentes à privacidade do usuário e à proteção de seus dados pessoais, hipótese de modificação dos termos de uso, disposições gerais e disposições finais, legislação e foro, disponibilização dos termos de uso em todas as plataformas, páginas, sites e aplicativos que contem com interação direta com o usuário, inclusão de mecanismos de comprovação do aceite do usuário quanto aos termos de uso das páginas, sites e aplicativos, manter as informações atualizadas em todos os termos de uso em páginas, sites e aplicativos mantidos pela organização dos quais haja interação direta por parte do usuário, uso de linguagem clara, acessível e de fácil compreensão para os usuários; uso de recursos que possibilitem ao usuário aumentar o tamanho da fonte do documento, de forma a facilitar a leitura e a compreensão por parte dos usuários; entre outros.*

mínimos de observação quanto a informações pormenorizadas pelos autores Larissa Lotufo, Leandro Bissoli e Rafael Siqueira[152].

### 3.3.11 Atualizações ou Confecções de Contratos, Políticas Internas, Código de Ética dos Algoritmos, Regulamento Interno, Acordos Comerciais e Termo de Sigilo e Confidencialidade (NDA)

Os documentos que envolvem as pessoas que tratarão de alguma forma os dados pessoais deverão passar por uma atualização à Lei 13.709/2018 e caso ainda não existam, devem ser imediatamente elaborados pelo Advogada Especialista.

Os principais documentos são os contratos de prestação de serviço ao cliente da empresa e com fornecedores; contratos de trabalho com os colaboradores; políticas internas que tenham delimitada a boa prática dos procedimentos em caso de ocorrência de algum incidente ou evento; o código de ética dos algoritmos no caso de empresas que trabalham com tecnologia e inteligência artificial; regulamento interno para explicar o que cada setor faz em relação aos dados pessoais transitados naquela empresa; acordos comerciais que possivelmente as empresas venham a ter com parceiros em recebimento ou transferência de dados pessoais dos seus clientes, ou de clientes dos seus clientes; e por último o termo de sigilo e confidencialidade dos dados e informações pessoais que pode ser assinado com clientes, colaboradores, prestadores de serviços e parceiros.

Os documentos supraelencados devem levar em consideração cada norma específica que aquela empresa segue como é o caso da ISO 27000[153] e em consonância com a LGPD destrinchar cada

---

[152]SLEIMAN, Cristina. ROCHA, Henrique. LOTUFO, larissa. BISSOLI, Leandro. SEMOLA, Marcos. TUPINAMBÁ, Marcos. SIQUEIRA, Rafael. **Segurança Digital: proteção de dados nas empresas**; organização Patrícia Peck Pinheiro. São Paulo: Atlas, 2021, p. 54-55.

[153] *As normas da família ISSO 27000 nasceram em 2006 e surgiram no mercado como uma medida de proteção e prevenção à segurança da informação das redes dentro do meio corporativo. [...]. Trecho retirado da obra SLEIMAN, Cristina. ROCHA,*

responsabilidade das pessoas, principalmente, operador e controlador, limitando assim, responsabilidades.

### 3.3.12 Treinamentos com a Equipe

Após as fases acima concluídas, a equipe que trata de dados pessoais precisa ser treinada, com questões de segurança da informação e conforme as estratégias montadas em cima dos pontos de vulnerabilidades e falhas encontradas.

### 3.3.13 Realização de Campanhas de Conscientização

É muito importante realizar campanhas de conscientização sobre a importância da LGPD nas empresas tanto no ambiente interno, quanto na promoção de ações educativas e informativas externamente, ou seja, ou público-alvo e à sociedade de maneira geral, como foi o caso do Banco Santander, que no capítulo anterior foi citada a campanha do "Santander *On*".

Outra empresa que também acertou na publicidade dessas campanhas e que atingiu o público em geral (sociedade) foi o Banco Bradesco, com a publicidade atrativa da família *Jetsons*[154].

Veja, que esta é uma forma atrativa de mostrar ao consumidor e até à novos clientes que o banco trabalha com inteligência artificial, e possui mecanismos de segurança dos dados pessoais de seus usuários.

---

*Henrique. LOTUFO, Iarissa. BISSOLI, Leandro. SEMOLA, Marcos. TUPINAMBÁ, Marcos. SIQUEIRA, Rafael. Segurança Digital: proteçao de dados nas empresas; organização Patrícia Peck Piheiro. São Paulo: Atlas, 2021, p. 46-47.*

[154] *Midia Interessante. Disponível em: <https://midiainteressante.com/2020/10/comercial-do-bradesco-futuro-os-jetsons.html>. Acesso 23/06/2021.*

### 3.3.14 Oferecimento de Suporte no Relacionamento com Clientes e com a Autoridade Nacional de Proteção de Dados (ANPD)

Ao Escritório de advocacia que for atender ao processo de *compliance* é indicado que tenha um departamento próprio composto por conciliadores, mediares e árbitros para que estejam preparados a atender possíveis demandas do contencioso gerada diretamente pelo titular dos dados buscando uma reparação do dano que lhe foi causado.

Desta forma, é possível minimizar os prejuízos financeiros e de imagem relacionados à algum evento de vazamento de dados pessoais, como foi o caso da empresa *Netshoes* que em um acordo pagou apenas R$ 500.000.00,00 (-)[155].

### 3.3.15 Início da Pesquisa de Satisfação

Tendo um cenário de implementação realizada pelo Advogado Especialista é indicado que se inicie pesquisas de satisfação com os clientes da empresa, para que se busque a efetividade da qualidade do serviço prestado.

É possível auferir o nível de eficácia que a implementação teve, pois o sucesso estará atrelado ao entendimento que as pessoas terão com relação a responsabilidade que cada um terá com a proteção de dados pessoais.

E o sucesso contínuo será responsabilidade da empresa que manterá o Advogado Especialista como *head* de operações que administrará o “Programa de *Compliance* LGPD do Brasil” por toda a existência da empresa.

.

[155] MPDFT e Netshoes firmam acordo para pagamento de danos morais após vazamento de dados. Disponível em: <https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2019/10570-mpdft-e-netshoes-firmam-acordo-para-pagamento-de-danos-morais-coletivos-apos-vazamento-de-dados>. Acesso 23/06/2021.

## CONCLUSÃO

Após analisar as diretrizes da Lei Geral de Proteção de Dados Pessoais e o antepassado legislativo que levou a disposição sobre a escrita desta nova lei, percebeu-se que não há efetividade da proteção de dados pessoais no Brasil.

Isto porque as normas que deveriam estabelecer direitos e deveres sobre o uso dos dados pessoais, em meio ao ambiente virtual, não acompanharam o avanço tecnológico que acabou por dar alcance a toda população brasileira de todas as classes sociais, inclusive as empresas que tratam dos dados pessoais, de pequeno a grande porte (nacionais e multinacionais brasileiras).

Dessa forma, a busca alucinada por escrever e disciplinar sobre o tema trouxe à tona uma legislação cheia de lacunas e anomalias que trarão resultados prejudiciais às empresas, além de uma falsa sensação de proteção aos titulares dos dados pessoais.

A LGPD surgiu como uma luz que prometeu segurança à proteção de dados pessoais de seus titulares, contudo, o ponto que daria desfecho à essa vigilância ainda está sendo formado, apenas tido como título de um capítulo que busca apenas a aplicação de sanção que tem, como resultado primeiro, o aumento financeiro (de arrecadação) destinado ao Poder Público.

## REFERÊNCIAS BIBLIOGRÁFICAS

ALEXY, Robert. **Teoria da Argumentação Jurídica**. A Teoria do discurso racional como Teoria da Fundamentação Jurídica. Rio de Janeiro, Forense, 2011.

ABPERITOS, 2020.
Disponível em: <https://abperitos.com.br/2019/10/09/exclusivo-detran-vaza-dados-pessoais-de-quase-70-milhoes-de-brasileiros/>, com acesso em 11.08.2020.

ATIENZA, Manuel. **As Razões do Direito – Teorias da Argumentação Jurídica.** Tradução de Maria Cristina Guimarães Cupertino. São Paulo: Landy Editora, 2006.

CORREIO BRASILIENSE. 2020. **General Heleno e o Vazamento de Dados.** Disponível em: <https://www.correiobraziliense.com.br/app/noticia/politica/2020/03/31/interna_politica,841485/ao-postar-exame-general-heleno-esquece-de-apagar-dados-pessoais.shtml>, com acesso em 23/09/2020.

DANTAS, Maria Augusta. **Bíblia Revisitada para Jovens**. Campinas: Bookseller, 2020.

DETRAN. 2020. **Detran vaza dados de CNH.**
Disponível em: http://www.detran;gob;br/Comunicacao/Noticias/23082020-Revolucao-tecnologica-e-desafios-da-pandemia-marcaram-gestao-do-ministro-Noronha-na-presidencia-do-aspx>, com acesso em 22/09/2020.

DIÁRIO POPULAR. 2021. O Tal do Questionário de Adequação. Disponível <https://www.diariopopulardesp.com.br/colunistas/post/o-tal-do-questionario-de-adequacao/566/>, com acesso em 23/06/2021.

DOWNEY, Roma; BURNETT, Mark. **A BÍBLIA — A História de Deus e Todos Nós**. São Paulo: Sextamte, 2014.

ESTADÃO. Notícia de vazamento de dados do General Heleno. Disponível <https://politica.estadao.com.br/noticias/geral,apos-piadas-na-internet-heleno-borra-dados-pessoais-de-resultado-de-coronavirus,70003255441>, acesso em 22/06/2021.

ÉPOCA NEGICIOS. Tecnologia: 84% das empresas brasileiras não estão preparadas para LGPD. Disponível < https://epocanegocios.globo.com/Tecnologia/noticia/2019/11/84-das-empresas-brasileiras-nao-estao-preparadas-para-lgpd.html>, acesso em 21/06/2021.

EUROPEAN CONVENTION ON HUMAN RIGTHS. Convenção Europeia dos Direitos do Homem. Disponível < https://echr.coe.int/documents/convention_por.pdf>, acesso em 22/06/2021.

FOUCAULT, Michel. **A Verdade e as Formas Jurídicas**. Tradução Eduardo Jardim e Roberto Machado. Rio de Janeiro: Editora Nau, 2013.

HABERMAS, Jurgen. **The Theory of Communicative Action**, v. I — *Reason and the Rationalization of Society; vol. II, Lifeworld and System: a critique of functionalist reason*; (1987), 152 p.; *Towards a communication-concept of rational collective will-formation. A thought-experiment, in Ratio Juris*, v. 2/2, julho 1988, p. 144-154, e a lúcida exposição de síntese de obra de WHITE (1995).

INSITORIS, Heinrich. O Martelo das Feiticeiras: Malleus Maleficarum, 17ª ed., Introdução histórica: Rose Marie Muraro, Prefácio: Carlos Byington, Tradução Paulo Fróes, Rio de Janeiro: Rosa dos Tempos, 2004.

G1. 2020. Disponível em: <https://g1.globo.com/sp/presidente-prudente-regiao/blog/psicoblog/post/2020/01/12/depressao-a-doenca-mais-incapacitante-de-2020.ghtml>, com acesso em 23/09/2020.

JORNAL DA RECORD. 2020. [Televisão na semana de 13 a 19 de setembro de 2020].

JORNAL OFICIAL DA UNIÃO EUROPEIA. Regulamento n. 1338/2008 do Parlamento europeu e do Conselho de 16/12/2008. Disponível <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32008R1338>, acesso em 22/06/2021.

JORNAL OFICIAL DA UNIÃO EUROPEIA. Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24/10/1995. Disponível <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046>, acesso em 22/06/2021.

JORNAL OFICIAL DA UNIÃO EUROPEIA. Regulamento EU 2016/679 do Parlamento Europeu e do Conselho de 27/04/2016. Disponível http://www.direitoshumanos.usp.br/index.php/Documentos-anteriores-%C3%A0-cria%C3%A7%C3%A3o-da-Sociedade-das-Na%C3%A7%C3%B5es-at%C3%A9-1919/declaracao-de-direitos-do-homem-e-do-cidadao-1789.html, acesso em 22/06/2021.

KEVIN ASHTON. 2020.
Disponível em: <https://en.wikipedia.org/wiki/Kevin_Ashton>, com acesso em 17/09/2020.

LINKEDIN. 2020 Disponível em: <https://br.linkedin.com/in/marcio-pugliesi-96924322>, com acesso em 23/09/2020.

LGPD DO BRASIL. Disponível <https://www.lgpddobrasil.com.br/>, acesso em 22/06/2021.

MALLEUS MALEFICARUM. Disponível <http://www.malleusmaleficarum.org/>, acesso em 23/06/2021.

MEZZETI, Luca; CÉZ, Joaquim Portes Cerqueira. **O Direito das Novas Tecnologias e o Ordenamento Constitucional**. Editora D'Plácido, 2019.

MÍDIA INTERESSANTE. Curiosidade, fotos, comunicação e marketing. Comercial do Bradesco traz mais uma vez "Os Jetsons". Disponível <https://midiainteressante.com/2020/10/comercial-do-bradesco-futuro-os-jetsons.html>, acesso em 22/06/2021.

MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS. MPDFT e Netshoes firmam acordo para pagamento de danos morais após vazamento de dados. Disponível <https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2019/10570-mpdft-e-netshoes-firmam-acordo-para-pagamento-de-danos-morais-coletivos-apos-vazamento-de-dados>, acesso em 22/06/2021.

NEVES, Daniel. 2020. **Holocausto.**
Disponível em: <https://brasilescola.uol.com.br/historiag/holocausto.htm>, com acesso em 12/08/2020.

PARLAMENTO EUROPEU. Proteção dos Dados Pessoais. Disponível <https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf>, acesso em 22/06/2021.

PLANALTO. CDC. Disponível < https://www.planalto.gov.br/ccivil_03/Leis/L8078compilado.htm>, acesso em 22/06/2021.

PLANALTO. Código Civil Lei 10.406 de 10/01/2002. Disponível < http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm>, acesso em 22/06/2021.

PLANALTO. Código de Processo Civil 13.105 de 16/03/2015. Disponível <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Lei/L13105.htm>, acesso em 22/06/2021.

PLANALTO. Código Penal. Decreto-Lei 2.848 de 07/12/1940. Disponível <http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848.htm>, acesso em 22/06/2021.

PLANALTO. Constituição Federal de 1988. Disponível <https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>, acesso em 22/06/2021.

PLANALTO. Decreto 10.474 de 26/08/2020. Disponível <http://www.planalto.gov.br/ccivil_03/_Ato2019-022/2020/Decreto/D10474.htm>, acesso em 22/06/2021.

PLANALTO. Lei 12.414 de 09/06/2011. Disponível <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>, acesso em 22/06/2021.

PLANALTO. Lei Carolina Dieckmann 12.737 de 30/11/2012. Disponível < http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm>, acesso em 22/06/2021.

PLANALTO. Lei Geral de Proteção de Dados Pessoais 13.709 de 14/08/2018. Disponível < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm>, acesso em 22/06/2021.

PLANALTO. Lei Complementar 105 de 10/01/2001. Disponível < https://www.planalto.gov.br/ccivil_03/Leis/LCP/Lcp105.htm>, acesso em 22/06/2021.

PLANALTO. Lei de Acesso à Informação 12.527 de 18/11/2011. Disponível <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm>, acesso em 22/06/2021.

PUBLICATIONS OFFICE OF THE EU. Regulamento 1338/2008 do Parlamento europeu e do Conselho de 16/12/2008. Disponível <https://op.europa.eu/en/publication-detail/-/publication/9661a3f5-1ee7-45be-a5b0-8435191f0963/language-pt/format-PDF>, acesso em 22/06/2021.

PUC. 2020. Aula de proteção de dados pessoais no curso de LGPD na instituição “Meu Curso” em janeiro de 2020.

PUGLIESI, Márcio. **Filosofia Geral e do Direito:** uma abordagem sistêmico-construcionista. São Paulo: Editora Oka, 2020.

SANTOS, Maria Celeste Cordeiro Leite dos. **Poder Jurídico e Violência Simbólica**. 1ª Ed. São Paulo: Editora Cultural Paulista, 1985.

SANTOS, Maria Celeste Cordeiro Leite dos (coord.); ARAÚJO, Marilene (org.). **O Novo Código de Processo Civil Brasileiro, um enigma a ser decifrado: percepções cognitivas na interpretação da norma**. São Paulo: Editora Max Limonad, 2016.

STRAUSS, Leo. **Direito Natural e História**. São Paulo: Martins Fontes, 2020.

TRATADO SOBRE O FUNCIONAMENTO DA UNIÃO EUROPEIA. Versao Consolidada. Disponível <https://eur-

lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF>, acesso em 21/06/2021.

REVISTA ABRIL. 2020. **Escândalo da Teoria da Conspiração Pizzagate**. Disponível em: <https://super.abril.com.br/mundo-estranho/pizzagate-o-escandalo-de-fake-news-que-abalou-a-campanha-de-hillary/>, com acesso em 17/09/2020.

SANTANDER. 2020. **Campanha Banco Santander On**. Disponível em: <https://www.santander.com.br/campanhas/santanderon>, com acesso em 21/09/2020.

SLEIMAN, Cristina. ROCHA, Henrique. LOTUFO, larissa. BISSOLI, Leandro. SEMOLA, Marcos. TUPINAMBÁ, Marcos. SIQUEIRA, Rafael. **Segurança Digital: proteção de dados nas empresas**; organização Patrícia Peck Pinheiro. São Paulo: Atlas, 2021.

SUPERIOR TRIBUNAL DE JUSTIÇA, 2020. Recurso Especial n. 1.457.199 - RS. Disponível em: <https://bdjur.stj.jus.br/jspui/bitstream/2011/114173/REsp1457199.pdf>, com acesso 23/09/2020.

TECHNOLOGY REVIEW. **O Novo Gerador de Linguagem GPT-3.** Disponível em: <https://www.technologyreview.com/2020/07/20/1005454/openai-machine-learning-language-generator-gpt-3-nlp/>, com acesso em 21/09/2020.

THE RIGTH TO PRIVACY. 2020. Disponível em: <https://pt.wikipedia.org/wiki/The_Right_to_Privacy_(artigo)>, com acesso em 22/09/2020.

TERRA. **Vivo e Governo de SP firmam acordo para controle da COVID-19**. Disponível : https://www.terra.com.br/noticias/coronavirus/vivo-e-governo-de-sp-firmam-acordo-para-controle-da-covid-19,133b7dcece13c62e128b6f6c361c75bc0ftrctgm.html, acesso em 16/16/2021.

UNICEF. Declaração Universal dos Diritos Humanos. Disponível < https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>, acesso em 22/06/2021.

UNIVERSIDADE DE COIMBRA. Informação Administrativa e Proteção de Dados. Disponível <https://www.uc.pt/protecao-de-dados/protecao_dados_pessoais/da_privacidade_a_protecao_de_dados >, acesso em 22/06/2021.

UNIVERSIDADE DE SÃO PAULO, 2020. **Biblioteca Virtual de Direitos** Humanos.
Disponível em: <http://www.direitoshumanos.usp.br/index.php/Documentos-anteriores-%C3%A0-cria%C3%A7%C3%A3o-da-Sociedade-das-Na%C3%A7%C3%B5es-at%C3%A9-1919/declaracao-de-direitos-do-homem-e-do-cidadao-1789.html>, com acesso em 22/09/2020.

VADEMECUM SARAIVA, 2020.

WIKIPÉDIA. 2020. **The Rigth To Privacy**.
Disponível em: <https://pt.wikipedia.org/wiki/The_Right_to_Privacy_(artigo)>, com acesso em 22/09/2020.

ZUFFO, João Antonio. **A Infoera: O Imenso Desafio do Futuro.** São Paulo: Editora Saber Ltda., 1997.

## FILMES

PRIVACIDADE HACKEADA. Filme, 2019. Disponível em:<https://www.netflix.com/br/title/80117542>. Acesso em 07/2019.

A ERA DOS DADOS. Filme, 2019. Disponível em:< https://www.netflix.com/br/title/81031737>. Acesso em 09/2020.

BLACK MIRROR. Filme, 2019. Disponível em:<https://www.netflix.com/br/title/70264888>. Acesso em 07/2019.