CADERNOS JURÍDICOS

DA FACULDADE DE DIREITO DE SOROCABA

FACULDADE DE DIREITO DE SOROCABA
FUNDAÇÃO EDUCACIONAL SOROCABANA

FUNDAÇÃO EDUCACIONAL SOROCABANA
FACULDADE DE DIREITO DE SOROCABA

Cadernos Jurídicos da Faculdade de Direito de Sorocaba

Cadernos Jurídicos da Faculdade de Direito de Sorocaba - Edição Especial – Direito Digital	**Ano 3 - n. 1**	**p. 1 - 210**	**2021**

FICHA CATALOGRÁFICA

Cadernos Jurídicos da Faculdade de Direito de Sorocaba – Edição Especial – Direito Digital - Ano III – n.1 (2021) – Sorocaba; SP: Faculdade de Direito de Sorocaba, Sorocaba, 2021.

Anual
Inicio: ano I, n.1 (2017)

1. Direito - periódico. I. Faculdade de Direito de Sorocaba, Direito.

CDU: 34(05)

Brígida Alves de Lima - CRB8/8724

Conselho Superior da Fundação

Diretoria do Conselho
Dante Soares Catuzzo Junior- Presidente
Iris Pedrozo Lippi
Noemia Celeste Galduroz Cossermelli
Luiz Antonio Zamuner

Suplentes
Adriana Tayano Fanton Furukawa
Eduardo Francisco dos Santo Junior
Luis Inácio Carneiro Filho

Conselheiros
Alexandre Dartanhan de Mello Guerra
Alexandre Ogusuku
Antonio Farto Neto
César Augusto Ferraz dos Santos
Diogo Corrêa de Morais Aguiar
Gustavo dos Reis Gazzola
Jorge Alberto de Oliveira Marum
José Augusto de Barros Pupin
José Eduardo Marcondes Machado
José Francisco Cagliari
José Pedro Zaccariotto
Paulo Sérgio Domingues
Welington dos Santos Veloso

Honorários
Gervino Cláudio Gonçalves
Rodrigo Maganhato

Diretor

Prof. Dr. Gustavo dos Reis Gazzola

Corpo Docente

Alexandre Dartanhan de Mello Guerra
Antonio Carlos Delgado Lopes
Antonio Paulo Ferreira de Castilho
Cássio Vinícius Dal Castel Veronezzi Lazzari Prestes
Celso Naoto Kashiura Júnior
Denis Donoso
Fernando Fernandes da Silva
Gilberto Carlos Maistro Junior
Gustavo dos Reis Gazzola
Gustavo Escher Dias Canavezzi
Hugo Leandro Maranzano
Iris Pedrozo Lippi
José Antonio Siqueira Pontes
José Augusto Fontoura Costa
José Eduardo Marcondes Machado
José Francisco Cagliari
José Pedro Zaccariotto
João Batista Martins César
Jorge Alberto de Oliveira Marum
Karen Cristina Moron Betti Mendes
Luis Inácio Carneiro Filho
Luis Mauricio Chierighini
Marcelo de Azevedo Granato
Mauro Augusto de Souza Mello Júnior
Mônica Miliani Martinez
Noemia Celeste Galduróz Cossermelli
Paulo Sérgio Domingues
Roberto de Campos Andrade Campos
Rubens José Kirk de Sanctis Junior
William Bedone

Secretária

Daniela de Campos Oliveira

CADERNOS JURÍDICOS DA FACULDADE DE DIREITO DE SOROCABA

Fundação Educacional Sorocabana
Rua Drª. Ursulina Lopes Torres, 123 – Jardim Vergueiro – 18030-103 – Sorocaba/SP
Sítio de Internet – https://www.fadi.br/portal/

NOTA DO DIRETOR DA FACULDADE DE DIREITO DE SOROCABA AO CADERNOS JURÍDICOS DA FACULDADE DE DIREITO DE SOROCABA

Dirijo-me à comunidade acadêmica para apresentar os Cadernos Jurídicos da Faculdade de Direito de Sorocaba – Edição Especial – Direito Digital 2021. Após as atividades em grupo de pesquisa coordenado pelo Professor Gustavo Canavezzi, titular da disciplina de Direito Digital, os discentes engajados no projeto dedicaram-se à elaboração de trabalhos escritos motivados pelos encontros e discussões estabelecidos nas aulas. Orientados pelo professor, os alunos aprofundaram-se nas leituras e na pesquisa jurisprudencial de modo a desenvolverem temas atuais situados na confluência entre a seara dos conhecimentos da informática e a ciência do Direito.

Embalados pelas descobertas intelectuais propiciadas primeiras pesquisas e pelo espírito de investigação despertado na faculdade, os alunos produziram seus textos inaugurais. É sobre estes artigos que os presentes Cadernos Jurídicos se voltaram de modo a propiciar a sua divulgação e permitir aos alunos a valorização de seu empenho bem como conferir aos jovens autores o incentivo tão necessário àqueles que iniciam a jornada. De se ressaltar a firmeza de propósito dos nossos alunos, que se lançam na vida intelectual no estudo de temas atuais e sobre os quais preponderam as interrogações sobre as certezas.

A palavra também é de agradecimento a todos que emprestam suporte editorial e administrativo aos Cadernos Jurídicos da Faculdade de direito de Sorocaba. A coordenação das publicações da Faculdade de Direito de Sorocaba, Cadernos Jurídicos e Revista, é tarefa realizada com a dedicação e capacidade organizacional do Professor Gilberto Maistro. A revisão dos textos, incumbência ao atento olhar da Professora Mônica Martinez. À Brígida, a tarefa de bibliotecária dedicada de conferir forma e atender às exigências das normas técnicas aplicáveis às publicações.

Felicito os autores e desejo-lhes fortuna nas publicações que se seguirão.

Dr. Gustavo dos Reis Gazzola

NOTA DO COORDENADOR DOS CADERNOS JURÍDICOS DA FACULDADE DE DIREITO DE SOROCABA

Tradição e modernidade não são realidades antagônicas. A tradição é construída pela via do trabalho sério, ardoroso e comprometido, em razão das conquistas alcançadas ao longo do tempo, resultados que trazem credibilidade e confiança. A modernidade, por sua vez, está na consciência e na atitude que deve ser verificada frente aos avanços que as novas técnicas e tecnologias trazem, tornando-se necessárias, pertinentes ou úteis a determinada atividade. Assim, devem ser estudadas e implantadas, a bem dos destinatários do processo desenvolvido.

A Faculdade de Direito de Sorocaba demonstra o acima afirmado. Há mais de seis décadas, a Faculdade de Direito de Sorocaba colabora com a história do ensino jurídico de qualidade. Nesse sentido, vale destacar que a Faculdade integra o seleto rol de Instituições de Ensino Superior agraciadas com o Selo *OAB Recomenda*, conferido aos *melhores Cursos de Direito* no Brasil – conquista obtida em diversas oportunidades. Sem dúvida, tradição e credibilidade sãomarcas da Faculdade de Direito de Sorocaba.

A tradição, contudo, não impediu a Faculdade de depositar a devida atenção e de agir no sentido de garantir ao corpo docente, ao corpo discente e aos integrantes do corpo técnico-administrativo condições estruturais de trabalho e estudo, com iniciativas voltadas à modernização de suas instalações e serviços. Além disso, nota-se o constante incentivo ao estudo dos temas mais candentes e dos impactos jurídicos das questões trazidas pelos avanços tecnológicos.

Nesse passo, merecem destaque relevantes iniciativas, como a introdução da disciplina *Direito Digital* no itinerário formativo na graduação, bem como o desenvolvimento de Grupos de Estudos na área, já com três ciclos anuais de atividades, no intuito de capacitar o alunado para o enfretamento de temas atuais e produzir conhecimento para compartilhar com toda a sociedade.

Justamente nesse campo, elogiável o trabalho do já mencionado Grupo de Estudos em Direito Digital, atualmente coordenado pelo Prof. Me. Gustavo Escher Dias Canavezzi, cujas pesquisas realizadas no terceiro ano (2020) resultaram em uma série de artigos científicos reunidos, agora, neste número especial dos *Cadernos Jurídicos* da Faculdade de Direito de Sorocaba.

Na atual edição, os *Cadernos Jurídicos* serão compostos integralmente por trabalhos produzidos por discentes do Curso de Direito da Faculdade de Direito de Sorocaba, membros do referido Grupo de Estudos, que merecem ser nominados: Lucas Francisco Camargo Munhoz,

Rafael Luiz Pio Santos Junior, Maria Eduarda Balera de Moraes, Júlia Mendes de Souza, Ana Paula Mello, Giovanna Coelho Miramontes, Sabrina Lumi Furucaba, Samanta Heloísa Carniato, Marta Prado de Albuquerque Sebastião, Juliana Torres Ferraz, Ian Matiello Grasso, Vinicius de Melo Alves, Maria Luiza Ruiz Orfali e Janine Evangelista.

O leitor encontrará, adiante, doze artigos, com estudos de questões de relevância jurídica, pertinentes à inteligência artificial e ao tratamento de dados. Para a *primeira edição especial dos Cadernos Jurídicos da Faculdade de Direito de Sorocaba,* nada melhor: a comprovação de que, no desenvolvimento de estudos jurídicos de qualidade, a tradição e a modernidade caminham unidas, a serviço da sociedade – legítima finalidade maior de toda produção científica.

A publicação dos *Cadernos Jurídicos*, nesta edição especial, concretiza, também, mais uma vitória da Faculdade de Direito de Sorocaba que, mesmo diante dos desafios trazidos pela pandemia, com responsabilidade e zelo pela saúde e pela vida de toda a sua comunidade acadêmica, prosseguiu com a sua missão e manteve-se firme no propósito de fomentar a pesquisa e difundir o conhecimento jurídico.

Registro, por fim, o relevante trabalho desenvolvido pelo Prof. Dr. Alexandre Dartanhan de Mello Guerra, para a publicação desta *edição especial*, e os agradecimentos ao Prof. Hugo Leandro Maranzano e ao Prof. Dr. Gustavo dos Reis Gazzola, Diretores da Faculdade de Direito de Sorocaba no período 2020-2021, pelo constante apoio à pesquisa e às publicações dos resultados obtidos pelos integrantes do corpo discente da Faculdade de Direito de Sorocaba.

Boa leitura e bons estudos!

Prof. Dr. Gilberto Carlos Maistro Junior
Coordenador dos Cadernos Jurídicos e da Revista da Faculdade de Direito de Sorocaba
Mestre (Universidade Metropolitana de Santos)
Doutor (Faculdade Autônoma de Direito) em Direito
Professor Titular de Direito Civil da Faculdade de Direito de Sorocaba
Advogado
gilberto.maistro@prof.fadi.br

NOTA DA COORDENAÇÃO DO GRUPO DE ESTUDOS EM DIREITO DIGITAL

A história nos deixa presentes e, entre os que são por ela deixados, determinadas pessoas, num determinado contexto marcam, não apenas medrando as bibliotecas com futuros alfarrábicos, mas rumando as naus humanas aos seus mais profundos anseios.

Foi nesse contexto que em 2020 realizamos o terceiro ano consecutivo do Grupo de Extensão em Direito Digital na Faculdade de Direito de Sorocaba, sem qualquer pretensão de exaurir a lógica e as estruturas trazidas pela Lei Geral de Proteção de Dados (Lei nº 13.709/2018 – LGPD), com um grupo muito especial de pessoas.

Estávamos diante da grande novidade legislativa, sem qualquer regulamentação infralegal, como a que teríamos com os guias orientativos de maio e outubro de 2021 pela ANPD e da Resolução CD ANPD n.º 1 de 28 de outubro de 2021, que regulamentou o processo de fiscalização e do processo administrativo sancionador da ANPD (Autoridade Nacional de Proteção de Dados).

A velocidade com que a tecnologia avança sobre as relações humanas exige estudos e interpretações que contém, pela natureza da disciplina, grande risco de se tornarem logo obsoletas. Portanto, os artigos produzidos são o resultado das pesquisas feitas no ano de 2020, antes mesmo da vigência da LGPD em 17 de setembro de 2020.

Essa lei, como as demais de nosso ordenamento jurídico, é um produto humano, histórico e político, ou seja, representa o resultado concreto da volição humana, atrelada à ideia de segurança e previsibilidade das relações humanas.

Metaforicamente, a ideia de segurança atrelada à sobrevivência pode ser comparada a um cavaleiro medieval e sua armadura. O cavaleiro medieval está seguro contra os duros golpes de seu adversário, protegido pela sua pesada armadura de metal. No momento da batalha, a armadura é útil e essencial; no entanto, ao atravessar um rio, caso caia da ponte, aquilo que outrora mostrou-se vital para sua proteção, agora é o seu túmulo e seu fim.

Todos que participaram do grupo tiverem que se despir das “armaduras” para enfrentar, de peito aberto, novas ideias e situações, não apenas sob a óptica teórica, mas também sob a perspectiva prática.

As pesquisas foram realizadas com o intuito de estudar o impacto da LGPD e as influências da GDPR (General Data Protection Regulation - Regulamento Geral de Proteção de Dados da União Europeia) no desenvolvimento do Direito Digital Brasileiro.

Tivemos a honra e felicidade em receber professores convidados que compartilharam seus conhecimentos com o grupo, de maneira direta e sem amarras. Agradeço o livre acesso às ideias e o carinho oferecido na transmissão do conhecimento, por profissionais internacionalmente reconhecidos, como o Prof. Sérgio Branco que nos trouxe reflexões sobrea memória e esquecimento na Internet; o Prof. Eduardo Magrani que nos presenteou com conhecimento sobre privacidade, tecnologia e cybersegurança; e o Prof. Maurício Guedes Pinto que nos apresentou aspectos práticos do governo digital, em especial o eSocial (trabalhista, previdenciário e tributário), antes mesmo da existência da Lei n.º 14.129/2021 (Lei do Governo Digital).

Registro meus sinceros agradecimentos à equipe de coordenação do grupo de estudos, em especial aos membros Rafael Luiz Santos Pio Júnior e Pablo Carvajal, que realizaram todas as atividades com atenção, presteza e dedicação, demonstrando um talento natural para a pesquisa e magistério.

É preciso que se registre um especial agradecimento aos colaboradores de nossa instituição, representados pela Sra. Brígida Alves de Lima, pois sem seu trabalho e dedicação esse projeto não seria possível.

Por fim, agradeço a todos os alunos e alunas do Grupo de Extensão em Direito Digital 2020 pela coragem no enfrentamento de temas tão novos e instigantes. São esses alunos que viverão nos castelos do amanhã, com uma tecnologia cada vez mais entranhada no tecido social. Parabéns a todos pelos primeiros passos dados rumo ao maior desafio da humanidade: o desenvolvimento tecnológico e seus reflexos.

Prof. Me. Gustavo Escher Dias Canavezzi

NOTA DA COORDENAÇÃO PEDAGÓGICA

Com imensa alegria recebo o convite para esta nota de apresentação de mais uma edição dos cadernos jurídicos da Faculdade de Direito de Sorocaba – FADI. Esta é mais uma das grandes conquistas que reforçam o compromisso da mais antiga Faculdade de Direito de Sorocaba e região com o crescimento da pesquisa científica e ensino jurídico de excelência.

Os cadernos jurídicos são frutos de intensa pesquisa de alunos e professores o que demonstra o comprometimento e a dedicação de toda comunidade Faculdade de Direito de Sorocaba, que em momento de pandemia e distanciamento social se superou apresentando diversos artigos científicos de enorme qualidade.

O sucesso deste trabalho, coordenado pelo Professor Doutor Gilberto Carlos Maistro Junior mais uma vez demonstra o comprometimento e empenho com o ensino jurídico de qualidade, que fez e faz da Faculdade de Direito de Sorocaba a melhor Faculdade de Direito de toda a região.

Não poderia também deixar de agradecer o apoio e incentivo do Diretor Prof.º Dr. Gustavo dos Reis Gazolla que tem trabalhado incansavelmente pelo fortalecimento de nossa Instituição e do Presidente da Fundação Educacional Sorocabana, o Advogado Dante Soares Catuzzo Junior, ex aluno Faculdade de Direito de Sorocaba. A vocês o meu muito obrigada por tudo que tem feito pela Faculdade de Direito de Sorocaba.

Os Cadernos Jurídicos da Faculdade de Direito de Sorocaba representam a forma como alinhamos a indissociabilidade entre ensino, pesquisa e extensão, honrando a tradição e o compromisso de quase sete décadas de ensino jurídico.

O propósito do projeto é promover a divulgação e o reconhecimento dos trabalhos desenvolvidos por alunas e alunos dos Grupos de Estudos e ainda oferecer material de pesquisa a toda comunidade jurídica.

Assim na certeza da importância da pesquisa para o desenvolvimento humano, esta nova edição dos Cadernos Jurídicos é motivo de alegria e satisfação para toda comunidade Faculdade de Direito de Sorocaba.

Profa. Dra. Patrícia Andrea Pannunzio Maranzano
Coordenadora Pedagógica da Faculdade de Direito de Sorocaba
Doutora em Educação e Mestre em Direito Constitucional.
Graduada em Direito pela Faculdade de Direito de Sorocaba
patricia.maranzano@fadi.br

NOTA DA PRODUÇÃO EDITORIAL

A edição especial dos Cadernos Jurídicos da Faculdade de Direito de Sorocaba – FADI é fruto do trabalho desenvolvido pelos alunos participantes do Grupo de Pesquisa em Direito Digital coordenados e orientados pelo Ilustre Prof. Me. Gustavo Escher Dias Canavezzi, o que reforça o firme propósito e compromisso da instituição com a pesquisa científica e ensino jurídico de excelência.

A publicação dos Cadernos Jurídicos demonstra o entusiasmo e dedicação de toda comunidade da Faculdade de Direito de Sorocaba, fruto do trabalho incansável dos alunos e professores superando todos os obstáculos e desafios desse momento histórico marcado pelo distanciamento social.

O sucesso deste trabalho é fruto da dedicação do Prof. Me. Gustavo Escher Dias Canavezzi, e ao incentivo e empenho dos Ilustres Professores Coordenadores Prof. Dr. Alexandre Dartanhan de Mello Guerra e Prof. Dr. Gilberto Carlos Maistro Junior, além do costumeiro apoio do Diretor Prof. Dr. Gustavo dos Reis Gazolla.

Os Cadernos Jurídicos da Faculdade de Direito de Sorocaba vêm alinhados aos princípios fundamentais que norteiam a Faculdade de Direito de Sorocaba, reconhece a indissociabilidade do processo ensino, pesquisa, extensão e honra a tradição de mais de seis décadas de ensino jurídico.

O propósito desta edição é promover a divulgação e o reconhecimento dos trabalhos apresentados pelos alunos no Grupo de Pesquisa em Direito Digital e ainda oferecer material de pesquisa a toda comunidade jurídica. E na certeza da importância da pesquisa para o desenvolvimento humano, a edição especial dos Cadernos Jurídicos é motivo de alegria e satisfação para toda comunidade Faculdade de Direito de Sorocaba.

Profa. Me. Karen Cristina Moron Betti Mendes
Coordenadora Núcleo de Prática da Faculdade de Direito de Sorocaba
Mestre em Direito pela Pontifícia Universidade Católica /SP
Graduada em Direito pela Faculdade de Direito de Sorocaba
Professora Titular de Prevenção e Resolução de Conflitos da Faculdade de Direito de Sorocaba
Advogada, Mediadora e Consultora Jurídica
karenbettimendes@gmail.com

SUMÁRIO

CADERNOS JURÍDICOS DA FACULDADE DE DIREITO DE SOROCABA – EDIÇÃO ESPECIAL – DIREITO DIGITAL – Ano 3 – n.1 - 2021

1. APLICAÇÃO DA INTELIGÊNCIA ARTIFICIAL NO JUDICIÁRIO BRASILEIRO
Lucas Francisco Camargo Munhoz e Rafael Luiz Pio Santos Junior 13

2. UMA BREVE ANÁLISE DA INTELIGÊNCIA ARTIFICIAL E SUA RELAÇÃO COM A RESPONSABILIDADE CIVIL
Maria Eduarda Balera de Moraes.....38

3. A RESPONSABILIDADE CIVIL E A IMPORTÂNCIA DA REVISÃO HUMANA NAS DECISÕES AUTOMATIZADAS PREVISTAS NA LGPD
Júlia Mendes de Souza 57

4. LGPD: AGENTES DE TRATAMENTO, RESPONSABILIDADE E ANPD
Ana Paula Mello e Giovanna Coelho Miramontes 73

5. O LIMITE DO TRATAMENTO DE DADOS SEM O CONSENTIMENTODO TITULAR
Sabrina Lumi Furucaba 81

6. REVISÃO E ATUALIZAÇÃO DE CONTRATO SOB O PRISMA DA PRIVACIDADE E PROTEÇÃO DE DADOS
Samanta Heloisa Carniato 95

7. PROTEÇÃO AOS DADOS DO USUÁRIO DE SERVIÇOS DIGITAIS PELALGPD E AS CLÁUSULAS ABUSIVAS NA POLÍTICA DE PRIVACIDADE"
Marta Prado De Albuquerque Sebastião 107

8. PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA
Juliana Torres Ferraz 121

9. RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAISNA LEI GERAL DE PROTEÇÃO DE DADOS: UMA BANALIZAÇÃO?
Ian Matiello Grasso 142

10. TUTELA COLETIVA E DADOS PESSOAIS
Marta Prado De Albuquerque Sebastião e Vinicius de Melo Alves.....175

11. APLICAÇÃO DA LEI Nº 13.709 DE 14.08.2018 E O DIREITO AO ESQUECIMENTO NOS DADOS DE NEGATIVAÇÃO SOB A ÉGIDE DO CÓDIGO DE DEFESA DO CONSUMIDOR
Maria Luiza Ruiz Orfali 190

12. LEI DA ANISTIA E O DEVER DE MEMÓRIA
Janine Evangelista 200

APLICAÇÃO DA INTELIGÊNCIA ARTIFICIAL NO JUDICIÁRIO BRASILEIRO

THE APPLICATION OF ARTIFICIAL INTELLIGENCE ON BRAZIL`S JUDICIARY SYSTEM

LUCAS FRANCISCO CAMARGO MUNHOZ[1]
RAFAEL LUIZ PIO SANTOS JUNIOR[2]

SUMÁRIO: 1. INTRODUÇÃO. 1.1. O que é Inteligência, Aprendizado e Memória. 1.2 Inteligência Artificial e Seu Funcionamento. 1.3 Como a IA funciona? 2. DESENVOLVIMENTO 2.1 Impactos da Inteligência Artificial na Sociedade. 2.2 Inteligência Artificial e o Poder Judiciário. 2.3 Reflexos da IA no Ordenamento Jurídico. 3. CONCLUSÃO. 3.1 Conflitos da Inteligência Artificial e o Ordenamento Jurídico Brasileiro. REFERÊNCIAS BIBLIOGRÁFICAS.

RESUMO

O presente artigo presta-se para responder a questionamentos acerca da influência, positiva ou negativa, que a Inteligência Artificial terá no ordenamento jurídico brasileiro, enquanto ferramenta de automação de tarefas e auxílio na tomada de decisões, bem como na atual composição do Estado Democrático de Direito, em um contexto estrutural e administrativo. Diante da perspectiva de crescimento exponencial do debate a respeito do tema, pretende-se ainda efetuar uma análise quanto ao modo como os algoritmos de inteligência artificial estão sendo implementados no Poder Judiciário, tanto em aspectos processuais quanto materiais do Direito. A partir dessa análise, é possível identificar em que situações e órgãos a Inteligência Artificial está sendo aplicada, de forma a impactar significativamente o poder de processamento do Judiciário, dissertando sobre as situações verificadas e teorizando a respeito de possíveis soluções que podem ser dadas aos problemas constatados, nos campos processual e administrativo.

Palavras-chave: Inteligência artificial; Poder judiciário brasileiro; Industria 4.0; Direito digital.

ABSTRACT

This article seeks to answer questions about negative or positive influences that the use of Artificial Intelligence may have in the Brazilian legal system while a automation tool and assist in decision making, as well as in the current composition of the Democratic State in a

[1] Advogado, Bacharel em Direito pela Faculdade de Direito de Sorocaba.
[2] Advogado, Bacharel em Direito pela Faculdade de Direito de Sorocaba.

structural and administrative context. Given the perspective of exponential growth of the debate on the subject, this article will analyze the way artificial intelligence algorithms are being implemented in the judiciary system, both in procedural and material aspects of law. Concluding to identify in which situations and which organs are being applied in Artificial Intelligence, and in what extent the AI is going impact the processing power of the Judiciary, disserting about the verified situations, theorizing about the possible solutions that can be given to the problems found in the field, procedural and administrative.
Keywords: Artificial Intelligence; Brazillian Legal System; Brazil`s Judiciary System.

1 INTRODUÇÃO

1.1 O que é Inteligência, Aprendizado e Memória

A inteligência tem sido definida, nos últimos anos, como a capacidade de alguém para a lógica, a leitura, a compreensão, o aprendizado, a comunicação e o planejamento. A palavra inteligência tem origem no Latim, advinda da palavra *intelligere*, que é composta por *inter= dentro*, e *legere= ler*. Portanto, com base na etimologia da palavra, inteligência é, estritamente, a capacidade de o indivíduo ler.

Contudo, conforme o avanço da psicologia nos estudos acerca da mente humana, a inteligência não é apenas ler, mas sim raciocinar, compreender, aprender. Howard Gardner, psicólogo norte-americano, desenvolveu a *teoria das múltiplas inteligências*, que, em síntese, aduz que a inteligência não é una, mas várias, subdividindo-se em 7 categorias:

> 1. Lógico-matemática é a capacidade de realizar operações numéricas e de fazer deduções.
> 2. Linguística é a habilidade de aprender idiomas e de usar a fala e a escrita para atingir objetivos.
> 3. Espacial é a disposição para reconhecer e manipular situações que envolvam apreensões visuais.
> 4. Físico-cenestésica é o potencial para usar o corpo com o fim de resolver problemas ou fabricar produtos.
> 5. Interpessoal é a capacidade de entender as intenções e os desejos dos outros e consequentemente de se relacionar bem em sociedade.
> 6. Intrapessoal é a inclinação para se conhecer e usar o entendimento de si mesmo para alcançar certos fins.
> 7. Musical é a aptidão para tocar, apreciar e compor padrões musicais.[3]

Dessa forma, levando em conta tal conceito, entendemos que inteligência é a capacidade de o indivíduo compreender e aprender. O aprendizado se dá através da

[3]"Quais são os oito tipos de inteligência? Superinteressante Abril.com." 4 jul. 2018, https://super.abril.com.br/mundo-estranho/quais-sao-os-oito-tipos-de-inteligencia/.

compreensão de algum fato informado. No momento em que um indivíduo lê um livro sobre ciência, por exemplo, este está adquirindo uma nova informação, processando-a e o seu cérebro compreende aquele fato. Esse conjunto de leitura, processamento e compreensão compõe o aprendizado.

Atualmente, com o advento da evolução tecnológica em razão da 4ª Revolução Industrial, os aparelhos comuns do nosso dia a dia, como celulares, relógios, geladeira e qualquer ferramenta que tenha ligação com a tecnologia se tornam "inteligentes". Mas por que o uso deste termo? Existe a capacidade de processamento de informações.

G*adgets* são "aparelhos tecnológicos"[4] e estão cada vez mais inseridos em nossa rotina, além de estarem cada dia mais conectados uns aos outros. Esses aparelhos têm a capacidade de receber alguma informação e processá-la, a fim de compreendê-la e realizar alguma reação.

Um exemplo muito comum é o corretor automático do teclado dos celulares. Os teclados vêm com uma configuração pré-estabelecida, uma *data base* contendo diversas palavras do idioma que é utilizado nele. Quando se utiliza alguma palavra desconhecida pelo programa, seja ela uma gíria ou alguma palavra escrita de maneira errada, o corretor automático processa aquela informação e entende que, comparando ela com sua base de dados, a palavra não existe e, portanto, deve ser corrigida.

Contudo, isso nada mais é do que uma mera reação a algo que está incompatível com aquilo que o *software* tem como paradigma. Acontece que, quando se ignora a sugestão do teclado e passa-se a utilizar aquela gíria frequentemente, o corretor "adquire" aquela expressão, incluindo ela ao seu dicionário. No momento em que se passa a usar a gíria continuamente, ocorre um processamento da informação (gíria), uma compreensão de que o usuário costuma utilizar aquela palavra e, por causa disso, esta deve ser incluída junto às informações. Percebe-se, portanto, que existe, inserida no *software*, a capacidade de aprender uma palavra nova e que ela não deve ser mais corrigida, pois é necessária ao usuário.

Cabe ressaltar que, de acordo com o dicionário Michaelis, aprender significa "compilação de informações"[5]. Então, a capacidade de o algoritmo compreender algo, como o exemplo dado acima, enquadra-se no conceito de inteligência.

[4]"O que é Gadget? E Widget, é a mesma coisa? - TecMundo." 16 abr. 2009, https://www.tecmundo.com.br/1959-o-que-e-gadget-e-widget-e-a-mesma-coisa-.htm.
[5] "Dicionário | Michaelis On-line - Uol." http://michaelis.uol.com.br/busca?id=OWQE.

Ainda utilizando o exemplo do corretor automático do teclado, a nova palavra por ele adquirida fica arquivada no armazenamento do dispositivo, tanto localmente, no armazenamento interno do dispositivo, parte esta que coloquialmente chamamos de "memória", como em bancos de dados de propriedade do desenvolvedor do software do teclado ou do dispositivo que utiliza aquele determinado software de digitação. Esses dados coletados, além de serem utilizados para aprimorar a experiência do usuário, corrigindo ou não com maior precisão, será utilizada para alimentar outros tantos bancos de dados, que alimentarão outras tantas ferramentas que se baseiam nesse tipo de aprendizado.)

A memória dos aparelhos varia dependendo da marca, do modelo e da utilidade, mas um aspecto comum entre todos é a capacidade do *gadget* de armazenar uma informação e sempre se lembrar dela, utilizando-a quando necessário. Essa capacidade de armazenar e utilizar informações foi e ainda é fator fundamental na criação, no desenvolvimento e no aprimoramento das ferramentas computacionais disponibilizadas à humanidade, isto é, o ser humano utiliza diariamente essa capacidade.

Quando lemos uma notícia sobre algum fato importante, essa informação fica armazenada em nossas mentes e, mesmo que se passe algum tempo, quando outro indivíduo perguntar algo sobre este assunto, saberemos falar sobre ele, pois o conteúdo que um dia estudamos ficou armazenado em nosso cérebro.

Por isso, é válido afirmar que a memória é o armazenamento de informações e fatos obtidos por meio de experiências ouvidas ou vividas. Relaciona-se fortemente à aprendizagem, que é a obtenção de novos conhecimentos, pois utiliza a memória para reter tais informações no cérebro.

Existem duas formas de adquirir e armazenar informações:

*Memória de Procedimento***:** utilizada para armazenar e verificar informações não verbalizadas como habilidades motoras, sensitivas ou intelectuais

Memória Declarativa: utilizada para armazenar e relembrar fatos e/ou dados recebidos pelos sentidos, criação de ideias, raciocínios que se subdividem em:

Memória Imediata: sua duração é de poucos segundos, pois ao utilizá-la é descartada pelo cérebro. Pode ocorrer armazenamento de tais dados inconscientemente.

Memória de Curto Prazo: sua duração é de poucas horas e por este fato pode haver perda de suas informações se caso ocorrer algum tipo de agressão ao cérebro.

Memória de Longo Prazo: sua duração pode chegar a anos de forma definitiva onde se encontra toda nossa autobiografia e conhecimento adquirido ao longo da vida. Para isso, o cérebro utiliza mecanismos de repetições, recordações e ideias associativas.

O sistema de memorização envolve as seguintes regiões: lobo temporal, neocórtex temporal, hipocampo, amígdala, tálamo, hipotálamo e córtex pré-frontal. Tais regiões cerebrais atuam como armazenadores que classificam fatos e eventos, estímulos sensoriais, respostas emocionais, resolução de problemas e comportamento.

Os computadores têm um sistema de processamento e armazenamento de informações muito parecido com o nosso. Eles possuem uma memória imediata e de curto prazo, a chamada *Random Access Memory*, mais conhecida como memória RAM. Do outro lado, possuem, também, memória de longo prazo, que servem para armazenar informações mais complexas e que necessitam estar sempre ao acesso do sistema; tal memória tem o nome de *Hard Disk*, comumente chamada de disco rígido ou HD.

Ao longo da evolução tecnológica, os desenvolvedores passaram a se espelhar muito no funcionamento do corpo humano para aprimorar suas criações, sempre buscando uma 'semelhança' para com o Homem, pois a ideia é se aproximar de um funcionamento idêntico ao do corpo humano.

Cabe ressaltar que o Homem procura cada vez mais desenvolver tecnologias que pareçam com o próprio ser humano. A partir dessa vontade, a ideia de uma máquina aprender se tornou o foco do estudo da Inteligência Artificial, utilizando complexos processos de coleta e tratamento de dados, para que a máquina pudesse aprender e compreender uma nova informação, e também memorizar o que absorveu de conhecimento, armazenando todas informações que foram obtidas por meio de dados em seu armazenamento interno ou em *cloud storage*. Tudo isso sempre voltado à ideia de criar máquinas inteligentes como o ser humano, as chamadas *machine learning*.

1.2 Inteligência Artificial e Seu Funcionamento

Antes de tratarmos a respeito do funcionamento da IA e de todo o seu impacto na sociedade atual, precisamos primeiro defini-la e entender seu funcionamento. O conceito de IA não será abordado sob a luz do conceito de inteligência multidisciplinar discorrido acima, mas sim levando em consideração o que a inteligência artificial realmente é para nós nos dias de hoje.

John McCarthy - considerado o pai da discussão sobre IA e criador da linguagem de programação (LISP), que permitiu que robôs jogassem xadrez com humanos, foi o primeiro a utilizar o termo Inteligência Artificial como definição para o campo da ciência e da engenharia voltado à criação e ao desenvolvimento de máquinas inteligentes. Tal definição era rasa, e pouco lapidada, tendo sido modificada ao passo que a revolução tecnológica avançava.

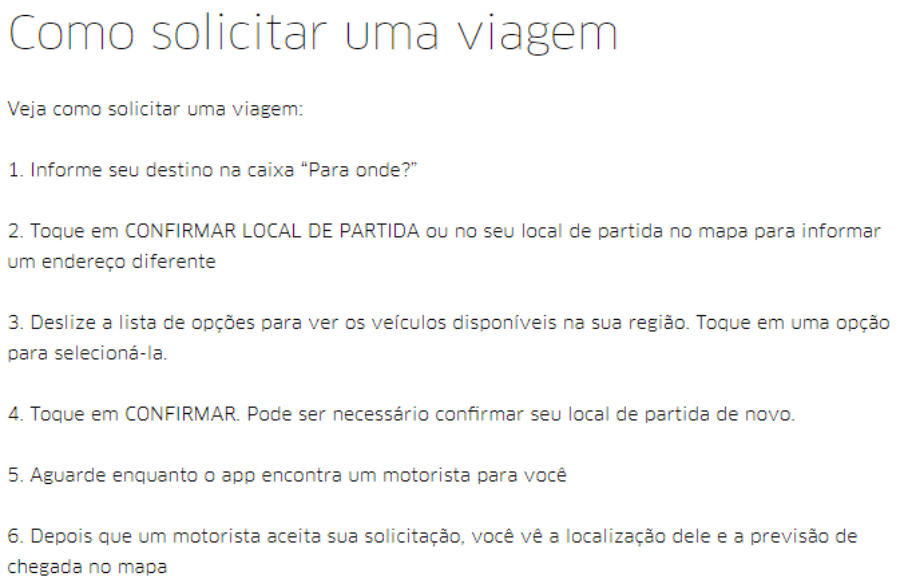
Ressalte-se que, ao tempo da "invenção" do termo, o conceito de informática era completamente diferente do que temos hoje. O computador como conhecemos mal podia ser imaginado, e sua finalidade computacional era completamente diferente da nossa.

Hoje, o poder computacional está amplamente difundido em nossa sociedade, tanto é que carregamos em nossos bolsos, usando o celular, milhares de vezes mais poderoso do que disponível no tempo em que se iniciou a discussão sobre IA.

Atualmente, o termo Inteligência Artificial continua descrevendo uma área da ciência e da engenharia voltada para o desenvolvimento de máquinas inteligentes, porém também tem sido utilizado com mais frequência para definir ou descrever a capacidade das máquinas em simular ou até mesmo replicar o comportamento humano, em qualquer área, em qualquer tarefa., Dessa forma, conforme se observará ao longo desse artigo, o termo é extremamente amplo, sendo utilizado dentro da comunidade científica para descrever desde o mais básico dos *algoritmos* utilizados nos aplicativos modernos, até mesmo a capacidade de realização de tarefas hoje consideradas extremamente complexas.

Com relação aos algoritmos, estes são o "*how to do*" do programa, ou seja, é a maneira com a qual o computador executará alguma função desenvolvida em seu código. Utilizamos algoritmos corriqueiramente em nosso dia-a-dia, por exemplo: se uma pessoa precisa se locomover de Sorocaba para São Paulo, existem 3 opções, sendo (i) ir de carro; (ii) utilizar ônibus intermunicipal; ou (iii) solicitar um motorista por meio de aplicativo. Caso a pessoa não tenha carro, restam-lhe duas opções, mas digamos que você está com pressa e, portanto, o ônibus seria demasiadamente ruim para sua locomoção. Tendo em vista a necessidade, você resolve solicitar um Uber e inicia o seu pedido. Você abre o aplicativo e digita o endereço do destino; escolhe a opção de carro; seleciona meio de pagamento; e por fim solicita o veículo para te levar até São Paulo.

Todos esses passos que explicamos são algoritmos que estão presentes em nosso cotidiano. A vontade de resolver as coisas faz com que tomemos algumas atitudes, utilizando a maneira mais lógica para se chegar até o resultado.



(*Imagem 1. Como Solicitar uma Viagem. https://help.uber.com/pt-BR/riders/article/como-solicitar-uma-viagem?nodeId=67f41961-e0aa-4670-af32-58be02c7c492*) [6]

É importante destacar que o “inteligente” dentro do termo IA se refere, em regra, a uma inteligência racional, de pensamento linear, sempre tendo sua aplicação voltada à análise, classificação e solução de um problema ou execução de uma tarefa qualquer. Via de regra, nem sempre os problemas ou as tarefas terão cunho matemático - a tarefa por exemplo pode ser a de sugerir uma palavra dentro de um contexto em que ela identifica, ou então seguir um caminho pré-determinado, como fazem os robôs seguidores de linha presentes em fábricas no mundo todo.

O fato é que a IA sempre tentará replicar/simular o comportamento humano, no sentido de analisar a situação apresentada a ela e buscar, dentro do seu “conhecimento”, qual é a melhor medida a ser tomada naquele momento, do ponto de vista exclusivamente racional, por enquanto. Importante dizer que a IA, ainda que não seja capaz de criar soluções inéditas, é capaz de enxergar padrões e soluções que os humanos não conseguem, e por isso é tão valiosa para o desenvolvimento tecnológico.

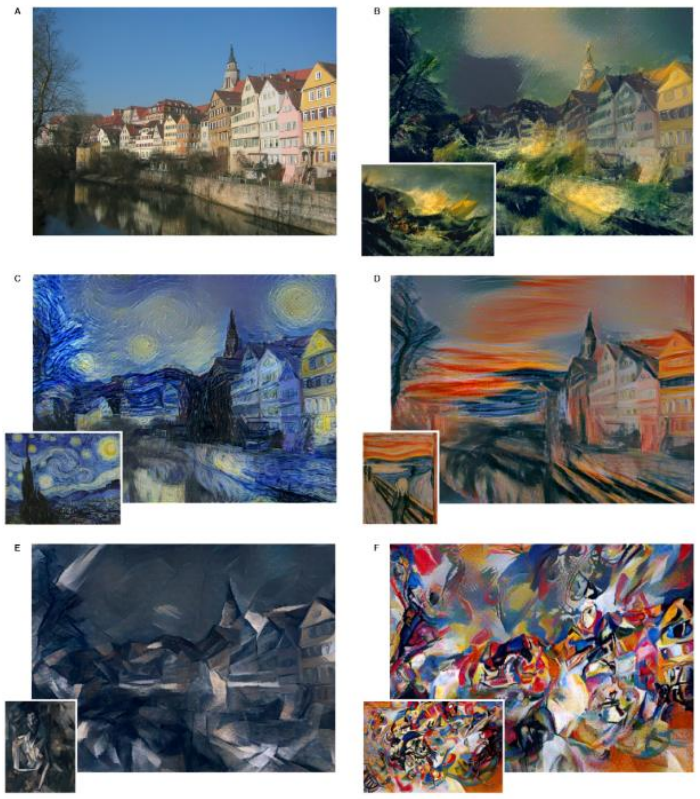
Quando se trata de IA, em relação daquelas que atuam diariamente interferindo em nossa rotina, qualquer outra inteligência, que não a lógico-matemática, é inexistente. Não é possível, por exemplo, ver o robô seguidor de linha citado no exemplo acima, parado em um

[6] "Como solicitar uma viagem | Ajuda para usuários Uber - Help | Uber." https://help.uber.com/pt-BR/riders/article/como-solicitar-uma-viagem?nodeId=67f41961-e0aa-4670-af32-58be02c7c492.

canto da fábrica, fazendo apontamentos e questionamentos sobre sua existência, ou tentando fazer qualquer outro tipo de tarefa que não seja aquele que ele foi programado para fazer.

Para toda regra, existem exceções e, portanto, existem situações nas quais a IA "desenvolve" espécies de inteligências variadas, como a interpessoal e até mesmo inteligência de cunho artístico. No entanto a base de fundo é puramente lógica-racional, motivo pelo qual se questiona se realmente, nos dias atuais, existe o desenvolvimento de uma inteligência que não a lógica, quando se trata de IA.

Há alguns exemplos que podem ser citados para relacionar com esse desenvolvimento, como a IA que pinta quadros, sendo ela alimentada com quadros do grande pintor *Van Gogh*; e também os inúmeros casos de *chatbots*[7], que foram colocados no mesmo ambiente para conversarem uns com os outros, e que ao final acabaram criando um idioma próprio, diferente daquele em que foram treinados.



[7] "[Chatbot] é um assistente que se comunica conosco através de mensagens de texto, um companheiro virtual que se integra em sites, aplicativos ou mensagens instantâneas e ajuda os empreendedores a se aproximarem dos clientes. Esse bot é um sistema automatizado de comunicação com os usuários." "What is a Chatbot and How to Use It for Your Business - Medium." 5jan.2018, https://medium.com/swlh/what-is-a-chatbot-and-how-to-use-it-for-your-business-976ec2e0a99f.

(*Imagem 2. A Neural Algorithm of Artistic Style Leon A. Gatys, Alexander S. Ecker, Matthias Bethge. august, 26, 2015. https://arxiv.org/pdf/1508.06576v1.pdf*)[8]

Observamos que nos casos apontados não existe "vontade" por parte da IA, ela foi treinada apenas para replicar, logo, no caso da IA pintora, seu aprendizado foi no sentido de reconhecer padrões nas pinturas fornecidas a ela, visando replicar tais padrões quando a ela for dado o comando para criar uma pintura Ainda que seja distinta do que já existe, essa pintura "inédita" tem o mesmo padrão do paradigma, isto é, a IA não consegue criar pintura com traços distintos daqueles que aprendeu, assim como não consegue transmitir emoções através da pintura, sendo essa uma característica importante da arte.

No caso dos *chatbots*, eles deixaram de usar o inglês e criaram novo idioma, não porque sentiram necessidade de criar uma língua própria, para identificar seu "povo", mas porque analisaram o idioma inglês, o contrastaram com o objetivo dado a eles - que era se relacionar - e ambos chegaram a conclusão que o inglês era uma língua extremamente ineficiente para a comunicação, passando então a usar linguagem própria. Este seria o caso de uma IA extremamente avançada e que, por ora, não está disponível a qualquer um, em qualquer lugar, pois não teria aplicação direta. Esse tipo de desenvolvimento visa apenas permitir o estudo de técnicas que venham aprimorar as tecnologias já existentes e que tenham aplicação direta. Veja que faltam à IA os elementos que mais nos tornam humanos, as emoções, a vontade.

Pois bem, respondida a pergunta "O que é IA?", agora precisamos entender como ela funciona.

1.3 Como a IA funciona?

Citamos acima que a IA sempre tentará replicar ou simular o raciocínio e pensamento humano, a fim de resolver problemas e desenvolver tarefas, de qualquer natureza. Com isso, seu funcionamento será bastante similar ao modo como construímos nosso pensamento e estruturamos nosso raciocínio.

Antes de discorrer sobre o assunto, é importante salientar que o objetivo neste tópico é apenas o de introduzir, de maneira muito simplificada e rasa, o funcionamento da IA, uma vez que se trata de um assunto complexo, que depende de conhecimento prévio a respeito do

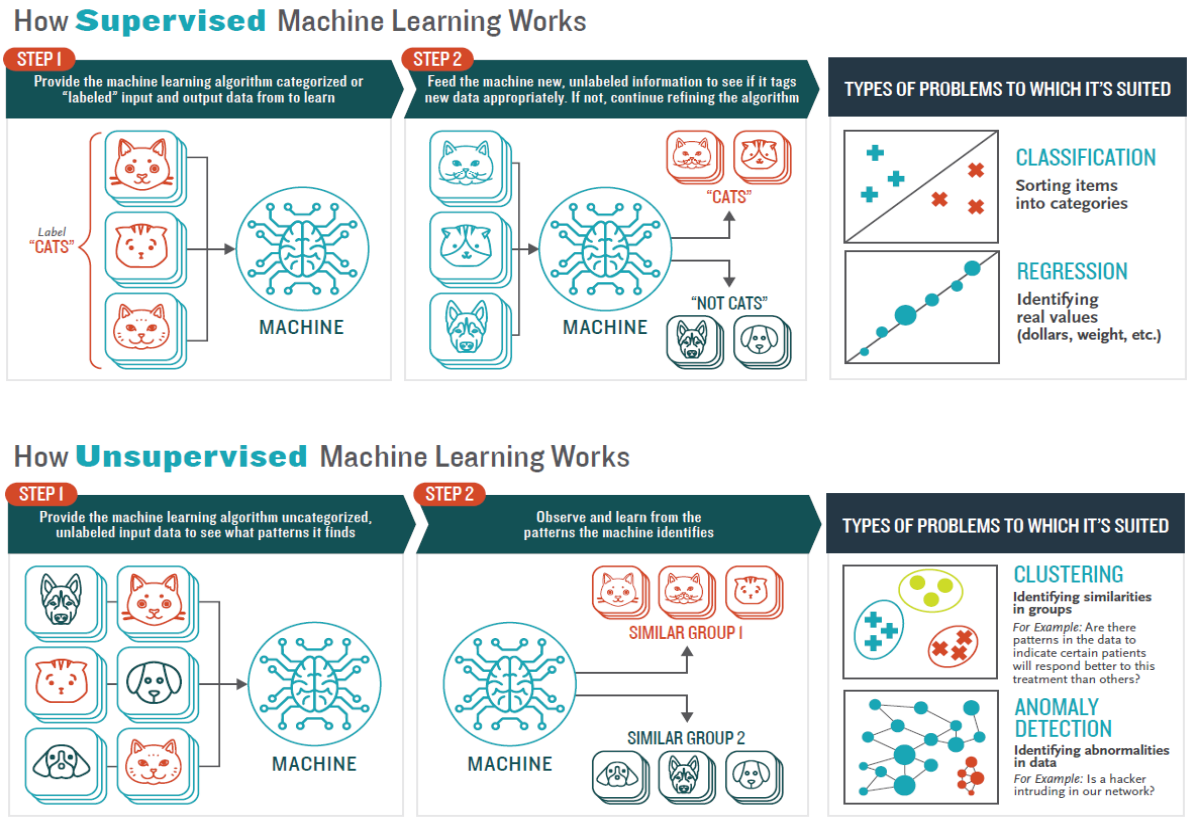
[8]"A Neural Algorithm of Artistic Style Leon A. Gatys, Alexander S. Ecker, Matthias Bethge. august, 26, 2015. https://arxiv.org/pdf/1508.06576v1.pdf

tema, e que, se abordado minuciosamente, seria contraprodutivo ao objetivo desse artigo científico.

O raciocínio e o aprendizado humano estão pautados nas informações que o ambiente nos fornece e com a IA não é diferente. Entretanto, existem diversos métodos de criar esse ambiente e alimentar a IA, sendo que aqui daremos atenção a apenas dois desses: Aprendizado Supervisionado e o Aprendizado Não Supervisionado.

No "Aprendizado Não Supervisionado", o algoritmo de classificação das informações recebe um conjunto imenso de dados para análise de padrões. O algoritmo, então, sem ter recebido qualquer tipo de instrução prévia, classifica em grupo os elementos que tenham padrões semelhantes. Ressalte-se que, nessa modalidade, a máquina não tem nenhum tipo de padrão pré-carregado para efetuar a classificação dos dados/elementos em grupos; é o próprio algoritmo que analisa os dados, percebe os padrões e os estabelece como paradigma para classificação.

No "Aprendizado Supervisionado", é fornecido ao algoritmo um conjunto paradigma de padrões para ser utilizado, ou seja, as informações dentro desse conjunto já estão padronizadas e classificadas, e a partir desse conjunto paradigma o algoritmo realiza a classificação dos demais dados que a ele forem fornecidos. A máquina, ao receber um novo elemento/dado, realiza uma análise deste, identificando suas características/padrões, e então compara com o conjunto paradigma. Se o elemento sob análise tem os mesmos padrões do paradigma, logo a máquina o classifica como sendo pertencente àquele grupo, e tudo o que divergir daquilo será classificado em um grupo distinto.



(*Imagem 3. A Quick Guide to How Machines Learn. Booz, Allen, Hamilton. https://www.boozallen.com/content/dam/boozallen_site/sig/pdf/publications/machine-intelligence-quick-guide-to-how-machines-learn.pdf*)[9]

Para ilustrar o que foi descrito, utilizaremos o Victor, projeto desenvolvido por estudantes da Universidade de Brasília, a UnB, e criado para identificar e classificar processos em temas de Repercussão Geral, no STF. Em determinado momento, percebeu-se a necessidade de identificar, dentro do processo, as peças-chave para classificação do processo como um todo.

Para dar início ao processo de identificação das peças dentro de um processo judicial, a equipe de direito do projeto teve de criar conjuntos paradigmas, classificando cada tipo de peça processual que precisaria ser identificada dentro do processo judicial, pelo Victor. Esses conjuntos, que possuíam informações a respeito do corpo textual e da identificação da peça, foram posteriormente utilizados para o treinamento do algoritmo classificador. Esse algoritmo passou a utilizar os padrões fornecidos pelo conjunto paradigma, para analisar a estrutura do

[9]A Quick Guide to How Machines Learn. Booz, Allen, Hamilton. https://www.boozallen.com/content/dam/boozallen_site/sig/pdf/publications/machine-intelligence-quick-guide-to-how-machines-learn.pdf

corpo textual de determinada peça dentro do processo e dizer se aquilo se tratava de Acórdão, Recurso Extraordinário, Agravo em Recurso Extraordinário, despacho, sentença ou outros.

Conforme o volume de dados fornecidos ao algoritmo através da análise de processos judiciais cresce, igualmente cresce a capacidade de indicar com maior precisão as peças processuais, uma vez que além dos padrões paradigmas fornecidos, o próprio algoritmo passa a analisar o processo em busca de padrões distintos, e que podem auxiliá-lo na identificação das peças processuais. É a junção do Aprendizado Assistido e do Não Assistido.

Com esses dados em mãos, o Victor pode fornecer à equipe de analistas do STF as informações de onde se encontra cada peça processual nos autos, para que possam proceder à análise dos requisitos de admissibilidade e, ainda, indicar, por análise própria do sistema, se aquele processo trata de Repercussão Geral ou não. Esta última parte dependerá do resultado de outras análises realizadas por outros algoritmos, diferentes do algoritmo que realiza a separação de peças.

Destacamos que, atualmente, o Victor em momento algum realiza qualquer juízo de mérito, bem como não profere nenhum tipo de decisão, de qualquer natureza. Ele apenas indica ao responsável pela separação de processos o tema de repercussão geral, quais são e quais não são.

2 DESENVOLVIMENTO

2.1 Impactos da Inteligência Artificial na Sociedade

Transporte, moradia, compras, marketing, entretenimento, todas essas áreas, e muitas outras, foram afetadas, sem dúvida alguma, pelo crescimento exponencial dos algoritmos de IA. Por trás de tudo isso, existe uma infinidade de situações que são obra de algoritmos que a cada dia se tornam mais avançados.

Grande parte do crescimento acelerado da presença de algum tipo de algoritmo inteligente se dá pela crescente necessidade de automatizar tarefas. Dirigir, lavar e passar roupas, e até mesmo checar o que está dentro da geladeira são tarefas que até alguns anos só poderiam ser realizadas por um ser humano, presentes fisicamente para executá-las, porém, com o avanço das ferramentas de IA, tal necessidade já está se tornando coisa do passado.

Imagine o seguinte cenário[10]. São 6 horas da manhã, o despertador toca, você tem que estar no trabalho às 8 horas em ponto. Sua casa já aprendeu - a partir da análise de seu

[10] The Social Web of Things - YouTube." 17 mar. 2011, https://www.youtube.com/watch?v=i5AuzQXBsG4.

comportamento e interação com os dispositivos da casa - sua rotina. Ela sabe quanto tempo você despende tomando banho, tomando seu café da manhã, e se organizando para ir ao trabalho (por isso ela te acordou às 6h). Você se dirige ao chuveiro, que liga automaticamente, assim que você entra no banheiro; Ao sair, suas roupas já estão passadas, você se veste e parte para a cozinha; Ao entrar pela porta da cozinha, a televisão liga, já sintonizada no canal que você costuma assistir; o café já está passado, pois enquanto você se vestia, sua lavadora já informou à cafeteira que você retirou as roupas passadas. Neste momento já são 7 horas, seu carro já sabe que houve um acidente na sua rota convencional até o trabalho[11], já traçou caminhos alternativos e já sabe quanto tempo você levará para chegar ao trabalho; ele sai da garagem e vai até a porta de sua casa, a qual te informa que seu carro já chegou, você pega suas coisas, entra no carro - no banco do passageiro, é claro - na central multimídia já estão sugestões de músicas. O carro te leva ao trabalho, te deixa na porta, com 10 minutos de antecedência, pois sabe que você não gosta de chegar atrasado. Perto do horário de sair, seu carro[12], que enquanto você trabalhava, buscou as crianças na escola e as deixou na casa dos avós, te aguarda, com a lista de alimentos que estão faltando em sua casa, uma vez que a geladeira e a dispensa te notificaram, bem como com a informação de qual o mercado com o menor preço.

Esse exemplo descrito acima não é imaginação, é realidade[13]. Com certeza não para todos, afinal, estamos no começo, o custo dessa tecnologia é altíssimo, porém, fato é que a tecnologia existe, e já está disponível ao público.

De todo a situação narrada, o exemplo do carro levar uma pessoa ao trabalho é o mais difícil de se ver aplicado rotineiramente, entretanto, isso se dá, principalmente, por dois motivos: falta de previsão legal e confiabilidade questionável de tais sistemas de condução autônoma existentes atualmente, que leva o fabricante de veículos a deixar esta função desabilitada por questões de segurança.

A Tesla já deu declarações nesse sentido, deixando claro que futuramente, assim que o sistema estiver pronto, seus carros receberão atualizações para habilitar os modos de condução autônoma plena, uma vez que atualmente essa autonomia é limitada propositadamente, exigindo na maioria das situações um humano presente, pelas questões

[11] The Social Web of Things II - YouTube." 17 mar. 2011, https://www.youtube.com/watch?v=z1Iq7nGRmiI.
[12]"Tesla says it will roll out Uber-style ride services program | Reuters." 20 out. 2016, https://www.reuters.com/article/us-tesla-rideservices-idUSKCN12K2IA.
[13] Paraimpu: a Platform for a Social Web of Things. Antonio Pintus, David Carboni, Andrea Piras. April 16. 2012 http://3s-cms.enstb.org/F2B506/wp-content/uploads/2013/02/2012-Pintus.pdf .

informadas. Inclusive, o CEO da Tesla, Elon Musk, já adiantou que está nos planos da empresa a possibilidade do veículo, enquanto não estiver sendo utilizado pelo proprietário, buscar parentes e amigos e disponibilizar o carro para uso destes, bem como realizar corridas, como uma espécie de concorrente direto do Uber e demais serviços de transporte e carona compartilhada.

Os carros possuem o Hardware[14], mas o Software ainda não é confiável o suficiente para liberá-lo ao público e permitir o uso de modo mais intenso, prova dessa capacidade é que atualmente os carros da marca são capazes de procurar vagas e estacionar sozinho, após o motorista deixar o veículo, bastando acessar o app e chamar o carro [15], para que ele saia de onde estacionou, e vá de encontro ao proprietário.

Deixando a automação residencial um pouco de lado, você, muito provavelmente, já se encontrou em uma situação onde pesquisou um assunto na web, ou apenas clicou em um link, e quase que imediatamente os anúncios das páginas que você costuma visitar passaram a exibir algum tipo de anúncio relacionado ao tópico que você acabou de pesquisar. Se você chegou até aqui, já deve imaginar que isso é obra de algum tipo de IA., e sim, você está certo. Isso é um exemplo dentro das incontáveis vezes com que interagimos de alguma forma com a IA., diariamente.

Atualmente promover uma marca, um evento ou um produto, se tornou extremamente fácil, basta criar uma página para o seu negócio no Facebook, fazer algumas publicações e utilizar a ferramenta de promoção para promovê-las e em questão de segundos um algoritmo entra em ação, sendo capaz de entender do que se trata o objeto alvo da promoção, e oferecê-lo para um perfil específico de pessoas, onde as chances de visibilidade e interação são quase que certas.

Dessa maneira, com um investimento baixíssimo (não existe valor mínimo, você investe o quanto quiser), pequenas e médias empresas, que não tem dinheiro para investir em grandes campanhas publicitárias, são capazes de alavancar suas vendas e crescer extremamente rápido, ainda mais quando ocorre a *viralização* [16] daquele anúncio.

Os últimos dados que temos sobre o impacto do Facebook na economia global e na brasileira são de 2015, e já naquela época, onde a ferramenta de promoção e outras, eram

[14]"Autopilot | Tesla." https://www.tesla.com/autopilot.
[15]"Summon Your Tesla from Your Phone | Tesla." 10 jan. 2016, https://www.tesla.com/blog/summon-your-Tesla-your-phone.
[16]"Entenda melhor o termo viralização: por que um conteúdo se torna" 19 mar. 2014, http://blog.penseavanti.com.br/entenda-melhor-o-termo-viralizacao-por-que-um-conteudo-se-torna-viral/.

menos refinadas e menos utilizadas, a plataforma, *segundo a pesquisa realizada* [17], era responsável pela injeção de 10 bilhões de dólares americanos no mercado brasileiro. É fato que o acesso facilitado a esse tipo de ferramenta e outras, muda a vida das pessoas.

Fica evidente, portanto, o impacto do uso da IA em nossa sociedade, causando mudança de hábitos, criando necessidades que antes não existiam. A tendência é de que cada vez mais tarefas deixem de exigir a presença de um ser humano para serem executadas, conforme a automação vai se tornando mais presente na sociedade. O tempo que antes era gasto com tarefas improdutivas poderá ser despendido de outras formas, seja no lazer, seja no trabalho.

O grande questionamento que surge a partir dessas ideias é a respeito da regulamentação de tudo isso. As leis e normas que regulam o convívio são um reflexo direto da sociedade e da forma como ela se organiza. Por isso, questiona-se se seria o Estado, com sua atual estrutura altamente burocrática, seja no Poder que for, capaz de acompanhar tais mudanças. O que será necessário para que o Estado não restrinja a capacidade evolutiva da sociedade?

2.2 Inteligência Artificial e o Poder Judiciário

A Inteligência Artificial também pode ser aplicada na área jurídica, atuando em diversos ramos do Direito, como, por exemplo, advocacia, magistratura, fórum.

Em países como Inglaterra e Estados Unidos, a IA já é de grande valia e auxilia os mais diversos profissionais da área na elaboração de petições, em pesquisas de jurisprudências, na elaboração de sentenças, no preenchimento de formulários e demais funções.

Em que pese o foco da IA não ser o Judiciário, seu uso tem crescido exponencialmente, surgindo até "advogados robôs", como o "*DoNotPay*" [18], criado por um jovem britânico, que já atuou em mais de 160 mil casos, auxiliando motoristas que se sentiram injustiçados por terem levado multas. Esse programa analisa o caso fazendo uma série de perguntas sobre o ocorrido e também sobre quem o requerente deseja processar para, em seguida, gerar os documentos necessários para o autor apresentar junto ao Tribunal e dar

[17]"Facebook divulga pesquisa sobre seu impacto na economia-Link" 20 jan. 2015, https://link.estadao.com.br/noticias/geral,facebook-divulga-pesquisa-sobre-seu-impacto-na-economia,10000029799.

[18]"Robot lawyer DoNotPay now lets you 'sue anyone' via an app " 20 jan. 2015, https://www.theverge.com/2018/10/10/17959874/donotpay-do-not-pay-robot-lawyer-ios-app-joshua-browder.

início ao processo. A frase usada pelo criador chamou a atenção dos usuários: “Processe qualquer um pressionando um botão”.

De acordo com os advogados Coriolano Camargo e Marcelo Crespo,

> Visto isso, é inegável que exista um enorme horizonte para a inteligência artificial, inclusive no âmbito legal e, portanto, muitas questões éticas e interesses permeando esta situação. Por exemplo, há sistemas desenvolvidos com base no computador cognitivo Watson da IBM. Um destes sistemas é o Ross, construído para atuar como advogado destinado a auxiliar com as pesquisas jurídicas e que se vale de aprendizagem mecânica e linguagem natural. [19]

Além da área da advocacia, a utilização de algoritmos no ramo da magistratura te, crescido. A título de exemplo, podemos citar o programa COMPAS, que atua como um auxiliar do juiz, analisando casos criminais e dando uma pontuação para o réu com base em sua vida, sua escolaridade, seus vínculos sociais, a utilização de drogas, os antecedentes criminais, a conduta, [etnia], a possibilidade de reincidência.[20]

O Compas utiliza os dados fornecidos para atribuir uma nota ao réu, classificando-o com baixo, médio ou alto risco de reincidência. O magistrado, por sua vez, como base, utiliza a análise entregue pelo algoritmo para sentenciar o indivíduo. Acontece que diversas decisões feitas pelo programa foram racistas, atribuindo notas mais baixas para pessoas negras. Em 2016, o jornal independente norte-americano ProPublica fez um estudo[21] de mais de 7 mil casos ‘julgados’ pelo Compas entre 2013 e 2014, e analisou os dois anos subsequentes dos réus que terminaram de cumprir suas penas, a fim de verificar a conduta de cada indivíduo, como o programa também faz.

O estudo concluiu que o algoritmo é duas vezes mais suscetível a denunciar erroneamente réus negros como possíveis reincidentes, se comparado aos réus de etnia branca. A matéria mostra cinco casos em que o indivíduo branco tinha antecedentes criminais piores e que, depois, vieram a cometer outros crimes em até dois anos após o cumprimento da pena, mas que foram classificados com pontuações mais baixas e com periculosidade considerada baixa, enquanto os condenados negros, por mais que tivessem antecedentes

[19]"Inteligência artificial, tecnologia e o Direito: o debate não pode" 30 nov. 2016, https://www.migalhas.com.br/DireitoDigital/105,MI249734,41046-Inteligencia+artificial+tecnologia+e+o+Direito+o+debate+nao+pode.

[20] "What Algorithmic Injustice Looks Like in Real Life" 25 maio. 2016, https://www.propublica.org/article/what-algorithmic-injustice-looks-like-in-real-life?utm_campaign=sprout&utm_medium=social&utm_source=facebook&utm_content=1464191771

[21]"Machine Bias— ProPublica." 23 mai. 2016, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

criminais mais brandos e não viessem a reincidir, o algoritmo os classificou com pontuações altas e os incluiu nos índices de maior periculosidade.

Para não ficarmos somente com exemplos estrangeiros, cabe ressaltar que o Brasil está avançando cada dia mais no uso da inteligência artificial. A empresa Magazine Luiza utiliza a "Lu" [22], uma IA com funcionalidade de *chatbot* que auxilia o consumidor em pesquisas no site da varejista. Já na área legal, grandes escritórios de advocacia têm usufruído de máquinas para automatizar os seus processos mais simples, como preenchimentos de formulários, cálculos processuais, elaboração de contratos e petições iniciais, como é o caso do escritório pernambucano "Advocacia Urbano Vitalino" [23], que utiliza o Watson, *software* desenvolvido pela IBM, para atuar no ramo advocatício.

Ainda na seara jurídica brasileira, vale lembrar que o Supremo Tribunal Federal, em 2018, passou a adotar o Victor, uma inteligência artificial desenvolvida pela Universidade de Brasília (UnB). Este programa tem a função de analisar os recursos que são enviados ao STF e classificá-los como sendo de repercussão geral ou não. O Victor tem capacidade de analisar e identificar todas peças processuais, convertendo-as em PDF para que seja possível extrair todo o conteúdo do documento e efetuar a classificação.

É válido ressaltar o comentário pelo Dr. Eduardo Magrani, coordenador do Instituto de Tecnologia e Sociedade do Rio (ITS Rio):

> "Com a internet, a gente usa inteligência artificial o tempo todo. Quando surge qualquer dúvida hoje, corremos para o Google. E o buscador do Google é uma inteligência artificial, ele trabalha com algoritmos. É que a gente tem uma ideia errada do que é Inteligência Artificial e não percebemos a presença dela no dia a dia"[24].

Percebe-se, portanto, que a inteligência artificial está se tornando cada dia mais presente na sociedade brasileira, inclusive no que tange ao judiciário. Em que pese estar havendo crescimento da aplicação de tal tecnologia, o debate acerca de questões éticas e limites não tem acompanhando o desenvolvimento da IA, faltando por parte da sociedade e dos juristas a discussão acerca do modelo ideal que se deve seguir para que evitemos abusos ou mau uso desta tecnologia.

[22]"Magazine Luiza — entrevista com o time responsável pela criação da" 20 mar. 2018, https://medium.com/botsbrasil/magazine-luiza-entrevista-com-o-time-respons%C3%A1vel-pela-cria%C3%A7%C3%A3o-da-lu-8fc987fbafad.
[23]"Inteligência artificial da IBM está ajudando escritório de ... - Canaltech." https://canaltech.com.br/inteligencia-artificial/inteligencia-artificial-da-ibm-esta-ajudando-escritorio-de-advocacia-brasileiro-106622/.
[24]"Máquina que pensa – Eduardo Magrani." 21 mar. 2018, http://eduardomagrani.com/maquina-que-pensa/.

2.3 Reflexos da IA no Ordenamento Jurídico

Saindo do campo técnico e focando mais nos aspectos jurídicos, é necessário ressaltar que a Inteligência Artificial terá, sobretudo, um forte impacto na seara legal, pois a tecnologia conflitará com diversos campos: civil, penal, administrativo, trabalhista, constitucional. Basicamente o reflexo da IA começa a partir de sua 'alimentação': *dados pessoais*.

Como explicado anteriormente, todo algoritmo necessita de uma base de dados ou de coleta de dados para que possa desenvolver sua rede neural e, futuramente, aprimorá-la. Tais dados serão essenciais para que o algoritmo possa desempenhar a sua função de maneira adequada. Como exemplo, podemos citar o Nubank[25], que analisa seu histórico de crédito, inadimplementos, Serasa, compras, salário, para decidir se irá conceder ou não o tão famoso "cartão roxinho". Se os dados utilizados pelo Nu não estiverem corretos, o algoritmo poderá decidir por não efetuar a liberação do cartão, pois os dados incorretos apontam você como um possível mau pagador, que, provavelmente, não honrará com o pagamento de eventuais faturas da empresa.

Antes de tratar propriamente das questões legais, deve-se ressaltar um novo fenômeno tecnológico que vem crescendo com o passar dos anos: a Internet das Coisas, ou IoT (*internet of things*). [26]

A relevância desse assunto está no fato de que a conexão de aparelhos inteligentes, como os *smartwatches*, gera bilhões de dados anualmente, e todos estes podem servir como base para que os algoritmos tomem suas decisões. A *Federal Trade Commission* (FTC), agência norte-americana, responsável pela proteção dos consumidores, manifestou sua preocupação com a IoT. "A FTC estima que cerca de 10 mil habitantes podem gerar 150 milhões de *data points* diariamente.", diz Eduardo Magrani em seu livro A Internet das Coisas (ed. 2018) [27].

Foi a partir do conhecimento dessa geração de dados e também dos escândalos de vazamentos, como o caso da Cambridge Analytica e o Facebook[28], que o Legislativo brasileiro deu andamento ao projeto de lei nº 53/2018, que hoje chama-se Lei Geral de Proteção de Dados (Lei nº 13.709/18). Tal Lei tem fulcro nos princípios constitucionais da

[25]"Nubank." https://nubank.com.br/.
[26]"The Panasonic laundry robot washes, dries, folds and Ideal Home." 1 set. 2017, https://www.idealhome.co.uk/news/panasonic-laundry-robot-seven-dreamers-180044.
[27]"[Livro] A Internet da Coisas – Eduardo Magrani." 17 mai. 2018, http://eduardomagrani.com/livro-internet-da-coisas-2018/.
[28]"Cambridge Analytica: tudo sobre o escândalo do Olhar Digital." 22 mar. 2018, https://olhardigital.com.br/noticia/cambridge-analytica/74724.

privacidade, dignidade da pessoa humana, isonomia, liberdade, e tem como fundamentos diversos aspectos, que são tratados em seu Art. 2º. Essa norma tem como finalidade a proteção dos dados pessoais de todos cidadãos brasileiros, a fim de evitar que o controlador e operador cometam abuso no tratamento dos dados fornecidos pelos usuários.

Retornando ao cerne deste artigo, o primeiro reflexo da inteligência artificial no ordenamento jurídico é com relação à proteção e tratamento de dados pessoais, englobando diversas áreas jurídicas. Podemos ressaltar também, que, na seara jurisdicional, a discussão acerca da legitimidade do uso de IA será importante, pois fere o princípio do juiz natural, visto que o trabalho tão somente da máquina não pode ser considerado como válido, devido ao fato de que as decisões devem vir de um magistrado.

Ademais, cabe questionar acerca do princípio da motivação das decisões judiciais, que se encontra no Art. 93, inciso IX, da Constituição Federal. Por mais que a decisão do algoritmo siga as fundamentações contidas em sua base de dado, ela é totalmente questionável, porque não foi analisada e redigida por um juiz, mas sim pela máquina. E se o magistrado viesse a analisar a decisão elaborada pela IA? Isso validaria a decisão automatizada?

A Lei Geral de Proteção de Dados (LGPD) traz, em seu Artigo 20, o chamado *right to explanation*, o direito à explicação, que se refere ao direito que o titular dos dados tem de solicitar uma revisão das decisões tomadas de maneira automatizada somente com base nos dados pessoais. Com base neste artigo da LGPD, abre-se um leque amplo para que o indivíduo solicite, sempre que necessário, revisões sobre quaisquer decisões automatizadas.

Esse direito é essencial, pois reforça a soberania que o titular tem sobre seus dados e que nenhuma decisão poderá ser tomada meramente com base nestas informações, evitando, assim, julgamento errôneos e tendenciosos, como vistos no caso do programa Compas. Entretanto, isso pode influenciar de maneira negativa o uso da inteligência artificial, porque sua aplicação servirá, principalmente, para uma resolução mais célere dos 80 milhões de processos judiciais que o Brasil possui. Ao invés de facilitar as decisões, poderá atrapalhar, já que as partes poderão peticionar pelo direito a explicação, fazendo com que o processo volte à estaca zero, isto é, dependendo tão somente da análise tradicional feita pelo magistrado e sua equipe.

A transparência, a ética e o bom senso serão pilares essenciais para que a IA possa ser aplicada de maneira correta no poder judiciário. A transparência será mais que essencial, pois será através dela que os magistrados e o CNJ encontrarão fulcro para a legitimidade e

segurança jurídica na utilização de algoritmos para auxiliar os juízes em suas decisões. Obviamente os 'juízes digitais' serão facilitadores, analisando os casos e produzindo decisões, com base nos julgados da respectiva vara e também dos tribunais de instâncias superiores, para que o juiz possa apenas analisar o caso concreto e perceber se tal sentença ou despacho está de acordo com as leis e jurisprudências. O mesmo questionamento aplica-se ao poder público, que não ficou de fora da lei de proteção de dados. A administração pública também encontra vantagens na automatização através de algoritmos, pois facilitaria muito a burocracia que se encontra instalada.

Diversos processos administrativos poderiam ser facilitados por meio do uso de inteligência artificial; licitações poderiam ser analisadas por máquinas que verificariam os pressupostos de validade e requisitos da contratação para o poder público; as burocracias internas dos órgãos públicos poderiam ser facilitados através da automatização de seus procedimentos; máquinas inteligentes poderiam facilmente organizar todo os arquivos de documentos, dando, assim, mais transparência às contas públicas, dentre outras possibilidade de aplicação.

Finalizando este tópico, cabe ressaltar um questionamento: o código fonte da inteligência artificial deverá ser público ou trata-se de segredo de negócio?

A Northpointe, desenvolvedora do Compas, foi objetiva, dizendo que não poderia informar aos réus a programação que utilizava para que a máquina decidisse, pois faz parte do seu *know-how* e, portanto, não divulgaram. Obviamente essa atitude feriu o princípio do devido processo legal, porque a falta de transparência dificulta o entendimento do raciocínio que levou àquela decisão. De acordo com o Drº Marcelo Crespo, "[...] é fundamental discutir e pensar criticamente sobre possíveis "arbitrariedades algorítmicas", ainda que com algum respaldo de decisões humanas." [29]

3 CONCLUSÃO

3.1 Conflitos da Inteligência Artificial e o Ordenamento Jurídico Brasileiro

Se formos falar exatamente do princípio do Juiz Natural e levá-lo à risca, seria possível a aplicação de IA ao poder judiciário? Após toda dissertação acima, é possível chegar a uma conclusão se a máquina realmente viciaria a decisão judicial? E um estagiário que faz sentença, isso seria semelhante à IA?

[29]"Algoritmos, reincidência e o Direito Penal. Crespo, Marcelo. 22, nov. 2016. http://www.academia.edu/30028483/Algoritmos_reincid%C3%AAncia_e_o_Direito_Penal.

O presente tópico é conclusivo, porém é válido levantar questionamentos, uma vez que o ordenamento jurídico (ainda) não está preparado para avanço tecnológico, muito menos para que este seja totalmente automatizado, como se espera em um futuro. Sabe-se que a jurisdição conta com 7 princípios norteadores, sendo eles: (i) investidura, (ii) aderência ao território, (iii) indelegabilidade, (iv) inevitabilidade, (v) indeclinabilidade, (vi) juiz natural, e (vii) inércia.

Tomando como base tais princípios, quais deles seriam mais mitigados se houvesse a aplicação da Inteligência Artificial? Algum seria extinto? Isso causaria alguma instabilidade jurídica? Será, a partir destes questionamentos, que iremos nortear a criação dos padrões de ética para a aplicação da IA no poder judiciário brasileiro.

Ainda que conclusivos, os tópicos acima e abaixo serão alvo de estudo específico em artigo futuro, visto que demandam estudos mais aprofundados que fogem ao objetivo inicial do presente artigo, qual seja introduzir o conceito de IA, explicar seu funcionamento e refletir a respeito de sua interação com a base do Direito, e, ainda, refletir a respeito dos impactos da automatização em nível processual.

Será que existe, hoje, uma ferramenta processual a fim de permitir o operador do direito, quem seja ele, requerer a revisão de eventual decisão proferida com base em sugestões de uma IA? Estaria o tribunal ou o magistrado que profere a decisão, pautada em "sugestões" de IA, obrigado a informar os critérios utilizados pela máquina para realizar o "julgamento"? Acreditamos que a resposta para ambos os questionamentos seja não, pelo fato de que a lei que regula, especificamente, a atuação de IA e de automação no Judiciário, (ainda) não existe.

Mesmo que a Lei[30] para contratação de empresas especializadas em promover a implementação e automatização do Judiciário e demais órgãos exista, ela é extremamente genérica, dando apenas diretrizes quanto à contratação de serviços, e não sobre a atuação da tecnologia na estrutura e no desenvolvimento do trabalho da administração pública, fato que nos leva a novo questionamento: qual é o limite da Administração Pública para a implementação de tais tecnologias? Como fica a segurança, não só jurídica, mas operacional do país? Como fica a segurança dos sistemas, uma vez que, certamente, a tecnologia não é, de forma alguma, à prova de falhas, bugs e vulnerabilidades que permitam ataques por hackers?

A prova de que os sistemas atuais podem ser facilmente hackeados se faz pelo constante e cada vez mais frequente vazamento de dados, os quais afetaram inclusive o CNJ -

[30]"D9283-Planalto." 7 fev. 2018, http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9283.htm.

Conselho Nacional de Justiça[31], recentemente, provocando vazamento de dados pessoais, e isso inclui CPF e número de contas bancárias de milhares de pessoas. Certamente que a tecnologia de automatização, no nível embrionário em que se encontra, é cheia de falhas e defeitos, que, sem dúvida alguma, serão exploradas por hackers. Ainda que se ateste eventual e remota impenetrabilidade dos sistemas responsáveis pelo tratamento de dados, sejam eles da Administração Pública, sejam eles de entes privados, a segurança nunca estará 100% garantida.

Tal afirmação se concretiza quando vemos notícias[32] a respeito de um suposto escândalo envolvendo grandes empresas de tecnologia, o FBI, a CIA, e o Governo Chinês, em que integrantes do Exército Chinês (Exército Popular de Libertação) estariam infiltrados em empresas que forneciam servidores e hardware para o governo americano e empresas como Amazon e Apple.

Estes infiltrados eram responsáveis por implantar nos citados equipamentos microchips que não eram parte do projeto original do equipamento vendido pela empresa envolvida no escândalo, e que permitiam a espionagem bem como a invasão remota de tais equipamentos. Ou seja, mesmo que o software dessas empresas de tecnologia e do Governo Estadunidense fosse impenetrável, a falha vinha do hardware e, portanto, era extremamente difícil de ser detectada pelos encarregados pela segurança do sistema, motivo pelo qual se levaram anos para descobrir tal falha.

Por fim, ainda que essa notícia tenha sido contestada por todos os envolvidos, e a prática maliciosa repetidamente negada pela empresa que tinha os equipamentos alterados pelos infiltrados, uma situação como essa, em um futuro próximo, no qual a tecnologia estará ainda mais presente em nosso cotidiano, seja ela nos órgãos públicos ou não, seria extremamente plausível.

REFERÊNCIAS BIBLIOGRÁFICAS

A., L. *et al.* A Neural Algorithm of Artistic Style. **Arxiv.** Disponível em: https://arxiv.org/abs/1508.06576v1.

AMARAL, F. E. O que é Gadget? E Widget, é a mesma coisa? **Tecmundo**. Disponível em:

[31]"Vazam dados do Conselho Nacional de Justiça; usuários e senhas" 1 abr. 2019, https://www.tecmundo.com.br/seguranca/140021-vazam-dados-conselho-nacional-justica-usuarios-senhas.htm.
[32]"The Big Hack: How China Used a Tiny Chip to Infiltrate ... - Bloomberg." 4 out. 2018, https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.

https://www.tecmundo.com.br/internet/1959-o-que-e-gadget-e-widget-e-a-mesma-coisa-.htm.

WHAT IS A CHATBOT AND HOW TO USE IT FOR YOUR BUSINESS. **Anadea inc.**, 2018. Disponível em: https://medium.com/swlh/what-is-a-chatbot-and-how-to-use-it-for-your-business-976ec2e0a99f.

ANGWIN, J. et al. Machine Bias. **Propublica.** Disponível em: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

ANGWIN, J. et al. What Algorithmic Injustice Looks Like in Real Life. **Propublica.** Disponível em: https://www.propublica.org/article/what-algorithmic-injustice-looks-like-in-reallife?utm_campaign=sprout&utm_medium=social&utm_source=facebook&utm_content=1464191771.

AUTOPILOT. **Tesla.** Disponível em: https://www.tesla.com/autopilot.

AXELSON, D. The Social Web of Things. **You tube**, 17 mar. 2011. Disponível em: https://www.youtube.com/watch?v=i5AuzQXBsG4.

AXELSON, D. Social Web of Things II. **You tube,** 15 de ago. 2012. Disponível em: https://www.youtube.com/watch?v=z1Iq7nGRmiI.

BLOOMBERG. The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. **Bloomberg**. Disponível em: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.

BOOZ; ALLEN; HAMILTON. A Quick Guide to How Machines Learn. **Boozallen** Disponível em: https://www.boozallen.com/content/dam/boozallen_site/sig/pdf/publications/machine-intelligence-quick-guide-to-how-machines-learn.pdf.

BRASIL. **Decreto Nº 9.283, de 7 de fevereiro 2018**. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9283.htm.

CALADO, C. Bots Brasil. Magazine Luiza - entrevista com o time responsável pela criação da Lu. **Médium**. Disponível em: https://medium.com/botsbrasil/magazine-luiza-entrevista-com-o-time-respons%C3%A1vel-pela-cria%C3%A7%C3%A3o-da-lu-8fc987fbafad.

COMO SOLICITAR UMA VIAGEM. **Uber b.v**. Disponível em: https://help.uber.com/pt-BR/riders/article/como-solicitar-uma-viagem?nodeId=67f41961-e0aa-4670-af32-58be02c7c492.

CRESPO, M. **Algoritmos, reincidência e o Direito Penal**. E-book. Disponível em: http://www.academia.edu/30028483/Algoritmos_reincidência_e_o_Direito_Penal.

CRESPO, MARCELO; CAMARGO, CORIOLANO A. A. **Inteligência artificial, tecnologia e o Direito: o debate não pode esperar!** E-book. Disponível em: https://www.migalhas.com.br/DireitoDigital/105,MI249734,41046-

Inteligencia+artificial+tecnologia+e+o+Direito+o+debate+nao+pode.

CUTMORE, A.; CUTMORE, A. **The Panasonic laundry robot washes, dries, folds and cleans your clothes**. Disponível em: https://www.idealhome.co.uk/news/panasonic-laundry-robot-seven-dreamers-180044.

GATYS, L. A.; ECKER, A.; BETHGE, M. **A Neural Algorithm of Artistic Style**. Disponível em: https://arxiv.org/pdf/1508.06576v1.pdf.

MAGRANI. Eduardo. A Internet da Coisas. **Eduardo Magrani**. Disponível em: http://eduardomagrani.com/livro-internet-da-coisas-2018/.

MAGRANI. Eduardo**.** Máquina que pensa. **Eduardo Magrani**. Disponível em: http://eduardomagrani.com/maquina-que-pensa/.

MOI&OACUTE; LI, J. Quais são os oito tipos de inteligência? **Superinteressante**. Disponível em: https://super.abril.com.br/mundo-estranho/quais-sao-os-oito-tipos-de-inteligencia/.

MUOIO, D. Tesla just made a big move to take on Uber. **Insider.** Disponível em: https://www.businessinsider.com/tesla-driverless-ridesharing-plans-could-take-on-uber-2016-10.

MUOIO, D. Uber once offered to partner with Tesla on self-driving cars - but Elon Musk said no. **Tesla.** Disponível em: https://www.businessinsider.com/tesla-elon-musk-decline-partnership-uber-self-driving-cars-2017-5.

Nubank, 2021. Disponível em: https://nubank.com.br/.

PINTUS, A.; CARBONI, D.; PIRAS, A. **Paraimpu: a Plataform for a Social Web of Things**. Disponível em: http://3s-cms.enstb.org/F2B506/wp-content/uploads/2013/02/2012-Pintus.pdf.

PORTER, J. Robot lawyer DoNotPay now lets you 'sue anyone' via an app. **The Verge**. Disponível em: https://www.theverge.com/2018/10/10/17959874/donotpay-do-not-pay-robot-lawyer-ios-app-joshua-browder.

SAGE, A. Tesla says it will roll out Uber-style ride services program. **Reuters**. Disponível em: https://www.reuters.com/article/us-tesla-rideservices-idUSKCN12K2IA.

SATURNO, Ares. Inteligência artificial da IBM está ajudando escritório de advocacia brasileiro - Inteligência Artificial. **Canaltech.** Disponível em: https://canaltech.com.br/inteligencia-artificial/inteligencia-artificial-da-ibm-esta-ajudando-escritorio-de-advocacia-brasileiro-106622/.

SUMARES, G. Cambridge Analytica: tudo sobre o esc. **Olhar Digital.** Disponível em: https://olhardigital.com.br/noticia/cambridge-analytica/74724.

SUMMON YOUR TESLA FROM YOUR PHONE. **Tesla**. Disponível em:

https://www.tesla.com/blog/summon-your-Tesla-your-phone?redirect=no.

TECNOLOGIA & MARKETING. Entenda melhor o termo viralização: por que um conteúdo se torna viral? **Avanti**, 2014. Disponível em: http://blog.penseavanti.com.br/entenda-melhor-o-termo-viralizacao-por-que-um-conteudo-se-torna-viral/.
UOL. **Michaelis moderno dicionário da língua portuguesa**. Disponível em: http://michaelis.uol.com.br/busca?id=OWQE.

VAZAM DADOS DO CONSELHO NACIONAL DE JUSTIÇA: USUÁRIOS E SENHAS. **Tecmundo**. Disponível em: http://www.tecmundo.com.br/seguranca/140021-vazam-dados-conselho-nacional-justica-usuarios-senhas.htm.

UMA BREVE ANÁLISE DA INTELIGÊNCIA ARTIFICIAL E SUA RELAÇÃO COM A RESPONSABILIDADE CIVIL

A BRIEF ANALYSIS OF ARTIFICIAL INTELLIGENCE AND ITS RELATIONSHIP TO CIVIL RESPONSIBILITY

MARIA EDUARDA BALERA DE MORAES[1]

RESUMO: 1. INTRODUÇÃO. 2. DA MÁQUINA DE ESCREVER AO COMPUTADOR. 2.1 História e Evolução da Máquina de Escrever. 2.2 História e Evolução dos Computadores. 3. INTELIGÊNCIA ARTIFICIAL: CONCEITO E FUNCIONAMENTO. 3.1 IA, a Ficção e a Realidade. 4. A RESPONSABILIDADE CIVIL NO DIREITO BRASILEIRO E NA UNIÃO EUROPEIA. 4.1 Responsabilidade dos robôs na União Europeia. 5. ATOS AUTÔNOMOS DA INTELIGÊNCIA ARTIFICIAL. 5.1. Nexo de Causalidade. 5.2 Hipótese de Exclusão da Responsabilidade. 6. PROVÁVEIS SOLUÇÕES A IMPUTAÇÃO DA RESPONSABILIDADE. 7. CONCLUSÕES. REFERÊNCIAS BIBLIOGRÁFICAS.

RESUMO

O presente trabalho tem como objetivo a breve análise da Inteligência Artificial (IA) e sua relação com a responsabilidade civil no âmbito do Direito Civil Brasileiro e da União Europeia, observando seus possíveis danos e consequências causados na sociedade. Dessa forma, serão abordados o funcionamento e a atuação autônoma (ou seja, sem a instrução de um ser humano) da Inteligência Artificial para então investigar a relação desses atos da IA e os danos causados, a fim de encontrar hipóteses que leve a um sujeito responsável pelas suas consequências. Outro ponto que será discutido neste trabalho, é que existindo um dano causado por atos autônomos da IA, há a necessidade de analisar o nexo causal da situação, observando qual o sujeito e se ele tem ligação direta com o ato que ocasionou no dano. E, por fim, tal debate fará surgir a questão da possibilidade da personalização da IA, logo, tornando os robôs sujeitos de direitos e obrigações.

Palavras-Chave*:* Responsabilidade civil; Inteligência artificial; Direito civil brasileiro; União Europeia; Nexo de causalidade; Danos imprevisíveis; Personalidade jurídica.

ABSTRACT

The present work aims to briefly analyze Artificial Intelligence (AI) and its relationship with civil liability in the scope of Brazilian Civil Law and the European Union, observing its possible damages and consequences caused in society. Thus, the functioning and autonomous performance (that is, without the instruction of a human being) of Artificial Intelligence will be addressed to then investigate the relationship of these AI acts and the damage caused, in order to find hypotheses that lead to a subject responsible for its consequences. Another point that will be discussed in this work is that if there is damage caused by autonomous AI acts, there is a need to analyze the causal nexus of the situation,

[1] Estudante do 5º ano diurno do curso de graduação em Direito na Faculdade de Direito de Sorocaba.

noting who the subject is and whether he has a direct connection with the act that caused the damage. And, finally, such debate will raise the question of the possibility of customizing the AI, thus making robots subjects of rights and obligations.

Keywords: Civil responsibility; Artificial intelligence; Brazilian Civil Law; European Union; Causality nexus; Unpredictable damage; Legal Personality.

1 INTRODUÇÃO

O termo "Inteligência Artificial" surgiu no ano de 1956 em um seminário que ocorreu em New Hampshire, a fim de estudar o aspecto de conhecimento ou outra característica da inteligência a qual poderia ser descrita ao ponto de ser construída por uma máquina para simulá-la[2]. Contudo, um dos principais marcos da Inteligência Artificial ocorreu em 1950, por Alan Turing, no chamado "Teste de Turing".

Turing publicou um artigo denominado por *"Computing Machinery and Intelligence" (Máquinas Computacionais e Inteligência)*, onde o mesmo expôs a capacidade da máquina de pensar e de ser inteligente[3]. Resumidamente, o teste consiste em dois seres humanos e uma máquina, onde um desses humanos será o interrogador e os outros serão testados pelo mesmo. Assim, divido por uma barreira, o ser humano (iremos chamá-lo de "A"), conversa com o outro ser humano ("B") e uma máquina de IA, assim, o humano "A" deverá distinguir quem é o "B"e quem é a máquina inteligente.

Após esses grandes marcos, a Inteligência Artificial vem crescendo cada vez mais e estando tão presente em nosso cotidiano que é impossível imaginar uma sociedade a qual não exista tal tecnologia. Dessa maneira, essa tecnologia vem adquirindo cada vez mais autonomiae desempenhando funções independentes de algum tipo de comando exercido pelo ser humano.

A Inteligência Artificial com toda a sua tecnologia permite que *softwares* imitem as redes neurais de um ser humano, a partir do uso do *machine learning (aprendizado de máquina)* – onde o uso de algoritmos que organizam dados e reconhecem padrões, fazem com que os computadores aprendam com esses modelos – e o *deep learning (aprendizado profundo)* – quetambém por meio de algoritmos, imita a rede neural do cérebro humano, reconhecendo imagense falas.

Toda essa tecnologia que envolve a IA, faz com que ela se torne autônoma dos comandos de nós seres humanos, conforme acima mencionado. Porém, com toda essa informação que foi obtida de forma independente pelos programas computacionais, podem

[2]Russell, Stuart J. (Stuart Jonathan), 1962. *Inteligência artificial*. Stuart Russell, Peter Norvig; tradução Regina Célia Simille. – Rio de Janeiro: Elsevier, 2013. Página 42.
[3]MAGALDI, Rodrigo. *O que é o Teste de Turing?* Disponível em: https://medium.com/turing-talks/turing-talks-1-o-que-%C3%A9-o-teste-de-turing-ee656ced7b6. Acesso em: 21 jun. 2020.

ocorrer decisões autônomas que causem danos para alguém, onde essas consequências não foram antes previstas pelos seus desenvolvedores.

Existindo um dano indenizável, surge também um sujeito responsável e uma relação jurídica, sendo assim, este trabalho tem como objetivo analisar esta problemática que ainda é repleta de dúvidas no âmbito do sistema jurídico de nosso país (como leis, jurisprudências e doutrinas) e pela União Europeia. Observa também o dano e o nexo de causalidade a fim de estudar as opções referentes a quem será o responsável pelas consequências causadas pelo sistema inteligente que age de forma autônoma.

Logo, será apresentado primeiramente a história e a evolução da tecnologia, como o surgimento da máquina de escrever até o computador e o conceito do termo "Inteligência Artificial", como essa tecnologia está sendo utilizada atualmente, bem como as possíveis consequências que poderão advir de seus atos autônomos e a análise do nexo de causalidade dos mesmos.

Por fim, será analisado a problemática do tema passando pelo entendimento jurídico utilizado pela União Europeia e chegando no Brasil, expondo também os níveis de interferência dos sujeitos nas consequências pelos atos da IA e se é possível haver uma solução para o embate, como a transformação de um robô para um sujeito de personalidade com direitos e deveres, por exemplo.

2 DA MÁQUINA DE ESCREVER AO COMPUTADOR

2.1 História e Evolução da Máquina de Escrever

Para poder chegar ao momento em que surgiu a IA e suas tecnologias, é importante que se compreenda toda a evolução de um sistema tecnológico que hoje se conhece como máquinas, computadores, robôs e outros milhares de objetos existentes. Ao se falar sobre IA logo se pensa que é imprescindível que exista, por exemplo, uma máquina por trás de seu surgimento, como um computador onde será utilizado para obter dados e transformá-los em *softwares* inteligentese autônomos.

Nesse mesmo raciocínio, é necessário também o estudo do momento anterior ao nascimento do computador a fim de tentar entender essa linha do tempo que será exposta, como as máquinas de escrever. A máquina de escrever foi um ponto de destaque ao estudar a história da tecnologia, sendo elas os melhores exemplos de como funciona uma evolução tecnológica, pois as primeiras existentes eram as maquinas mecânicas, se transformando em eletromecânicas e, por fim, as elétricas (mais tecnológicas).

A primeira tentativa de construir uma máquina de escrever foi feita em 1714, por Henry Mill, seguindo até a data de 1829, onde o inventor William Austin Burt inventou a primeira máquina com os caracteres colocados em uma roda semicircular que girava e imprimia no papel[4]. Já na metade do século XX, as máquinas elétricas e portáteis já estavam presente no cotidiano das pessoas, sendo essas mais desenvolvidas e sofisticadas.

Existindo a necessidade de ter uma escrita rápida e eficiente, as máquinas de escrever logo se tornaram indispensáveis as empresas, bancos, escritórios. Contudo, com a expansão cada vez maior, teve sua "extinção" e substituição pelos computadores.

2.2 História e Evolução dos Computadores

O termo "computador" surge do verbo "computar", remetendo a ideia de que as primeiras máquinas eram feitas com essa finalidade. O "ábaco" é considerado o primeiro computador criado há mais de 2.500 a.C, se tratando de instrumento mecânico que realiza operações algébricas. Após o ábaco, surge outras máquinas, como: a primeira máquina de calcular mecânica em 1642, por Blaise Pascal[5]; a Máquina Diferencial feita em 1822, que era capaz de resolver equações polinomiais, possibilitando a construção de tabelas de logaritmos ea Máquina Analítica feita em 1823, dispositivo capaz de resolver qualquer tipo de cálculo, contanto que fosse devidamente programado para isso, ambas por Charles Babbage[6].

[4]MOUTINHO, Célia. Gabinete do Património Histórico da Caixa Geral de Depósitos Setembro de 2011. Disponível em: https://www.cgd.pt/Institucional/Patrimonio-Historico-CGD/Estudos/Documents/Maquinas-de-escrever.pdf. Acesso em: 24 jun. 2020.
[5]SOBRAL NUNES, Sérgio. *Introdução aos Computadores. Computadores e Redes de Comunicação Mestrado em Gestão de Informação*, FEUP 06/07. Disponível em: https://web.fe.up.pt/~ssn/disciplinas/crc/computadores.pdf. Acesso em 24 jun. 2020.
[6]SARAIVA, Márcio. *Um "exame de DNA" na carreira de dois grandes cientistas para descobrirmos o "pai" da nossa profissão*. Disponível em: http://www.dsc.ufcg.edu.br/~pet/jornal/agosto2009/materias/carreira.html. Acesso em: 24 jun. 2020.

Importante destacar também o famoso matemático Alan Turing, que aos seus 24 anos de idade criou uma máquina que poderia imitar qualquer sistema formal. Outra invenção de Turing foi o desenvolvimento de um teste onde um usuário "A" deveria conseguir diferenciar uma resposta de suas perguntas estavam sendo feitas por um computador ou pelo usuário "B", caso o teste fosse afirmativo, a máquina era considerada dotada de inteligência artificial[7].

Logo, tem-se um breve resumo do começo da linha do tempo do computador, saltando para as próximas fases intituladas como as gerações (primeira, segunda, terceira e quarta). A Primeira Geração do computador surgiu em 1946, com a inauguração do computador ENIAC[8], sendo esse a máquina mais rápida feita até então, resolvendo cinco mil adições e subtrações, por exemplo.

A Segunda Geração foi marcada pelas novas máquinas, dentre elas o IBM TX-0 (1958) que tinha um monitor de vídeo de primeira qualidade e possuía até mesmo um dispositivo de saída sonora. Já a Terceira Geração são os computadores da década de 60, tendo como exemploo Burroughs B-2500 que armazenava milhões de números, enquanto o ENIAC apenas vinte.

E, por fim, a Quarta Geração que se figura até os dias atuais e é caracterizada pelo maior aperfeiçoamento da tecnologia, onde é proporcionado uma otimização da máquina para os problemas dos usuários em nanosegundos[9].

3 INTELIGÊNCIA ARTIFICIAL: CONCEITO E FUNCIONAMENTO

Após uma breve introdução à linha do tempo da tecnologia, chega-se ao surgimento da Inteligência Artificial e das tecnologias que ajudam em seu desempenho.

Segundo o dicionário, a palavra "inteligência" pode significar "faculdade de conhecer, de compreender: a inteligência distingue o homem do animal" e "artificial" é descrita como

[7]Frisa-se também, outra invenção de Alan Turing que gerou até mesmo um filme chamado "O Jogo da Imitação", a qual foi projetado por ele em 1943, a Colossus, um computador que quebrava os códigos nazistas secretos (considerados impossíveis de decifra-los), conseguindo vencer os códigos alemães e prestando grandemente sua ajuda para a Segunda Guerra Mundial.

[8]Electronic Numerical Integrator and Computer (ENIAC - em português: computador integrador numérico eletrônico) foi o primeiro computador digital eletrônico de grande escala. O ENIAC começou a ser desenvolvido em 1943 durante a II Guerra Mundial para computar trajetórias táticas que exigiam conhecimento substancial em matemática com mais agilidade, mas só se tornou operacional após o final da guerra. - https://pt.wikipedia.org/wiki/ENIAC.

[9]https://www.ime.usp.br/~macmulti/historico/histcomp1_12.html.

aquilo “que é produzido não pela natureza, mas por uma técnica”. Somando os termos “inteligência” e “artificial”, resulta no que, para o autor Blay Whitby: “estudo do comportamento inteligente (em homens, animais e máquinas) e a tentativa de encontrar formas pelas quais esse comportamento possa ser transformado em qualquer tipo de artefato por meioda engenharia”[10].

Assim, a IA surge com o avanço da tecnologia, recebendo esse nome pela primeira vez por John McCarthy, em 1956 no campus Dartmouth Colege, durante um seminário de oito semanas. Os especialistas que frequentaram esse seminário acreditavam na construção de computadores para desempenhar tarefas ligadas à cognição, abstração e uso de linguagem[11]. Desde então, a IA cresce mais e mais, se tornando ainda mais inteligente e participativa no cotidiano das pessoas.

Em uma linguagem leiga e de fácil entendimento, a Inteligência Artificial nada mais é que um agrupamento de códigos e dados, onde os primeiros leem e interpretam os segundos, ou seja, a IA nasce desse procedimento de análise de dados, os quais são gerados pela chamada*big data*[12]. Para o autor Magrani, *big data* se trata de um “termo em evolução que descreve qualquer quantidade volumosa de dados estruturados, semiestruturados e não estruturados que tem o potencial de serem explorados”[13].

Portanto, a *big data* é de grande influência para o funcionamento da Inteligência Artificial, onde esse armazena e processa dados que surgem do dia a dia das pessoas, como qual caminho alguém faz todos os dias para lhe dar a informação privilegiada de quanto tempo irá levar até chegar ao destino de sempre. Além da *big data*, outras tecnologias são utilizadas parao funcionamento da IA, como o *machine learning, o deep learning*[14] e o Processamento de Linguagem Natural (PLN)[15].

O *machine learning* é a capacidade de os computadores tornarem capazes de aprender e evoluir, ocorrendo um processamento lógico dos dados e a identificação de padrões que geram

[10]WHITBY, Blay. *Inteligência artificial: um guia para iniciantes; tradução de Cláudio Blanc.* São Paulo: Madras,2004.

[11]Época Negócios Online. Leia o texto do convite que criou o termo inteligência artificial**.** Disponível em: https://epocanegocios.globo.com/Tecnologia/noticia/2019/03/leia-o-texto-do-convite-que-criou-o-termo-inteligencia-artificial.html. Acesso em 28 jun. 2020.

[12]Sua tradução pode se dar como “grandes dados”.

[13]A internet das coisas. Eduardo Magrani. — Rio de Janeiro: FGV Editora, 2018.

[14]*Machine Learning* e *deep learning* tem sua tradução, respectivamente, como “aprendizado de máquina” e “aprendizado profundo”.

[15] Não se pode deixar de citar também a Internet das Coisas, a qual contribui muito à Inteligência Artificial, fazendo com que os dados sejam ainda mais aprimorados e as máquinas ainda mais inteligentes.

então a inteligência[16]. Já o *deep learning* é a tentativa, se assim pode dizer, da imitação da rede neural do cérebro humano na forma de algoritmos, o que faz com que aprenda sobre uma determinada área com pouco ou nenhuma supervisão[17]. E, por fim, o Processamento de Linguagem Natural (PLN), é o responsável pela naturalização e humanização dos robôs, encontrando padrões e reconhecendo a linguagem natural.

Toda essa tecnologia remete a uma maior autonomia das máquinas, pois, acabam se tornando mais inteligentes e não necessariamente precisam de comandos vindos de seres humanos, mas agindo com autonomia. Na área da ficção científica, é natural haver máquinas autônomas – como os robôs - que dominam o mundo e que se rebelam contra a humanidade, fazendo os telespectadores questionarem se um dia isso será possível.

3.1 IA, a Ficção e a Realidade

Quando se fala em ficção, a Inteligência Artificial e os robôs estão presentes em diversos filmes, jogos e séries, como o programa de televisão *Black Mirror*[18], onde basicamente todos os seus episódios contém tecnologias avançadas e IA. Um episódio bastante marcante e que será de grande auxílio para o entendimento desse projeto, é o "*Crocodile"*[19], narra a história secundária de um veículo de pizzas, autônomo e dotado de inteligência, que atropela um pedestre e o mesmo acaba sofrendo uma lesão em seu braço, levando a necessidade da empresa de seguros averiguar o caso e descobrir se a máquina teve ou não responsabilidade sobre o acontecimento.

Tal série de televisão é apenas um dos inúmeros exemplos que existem sobre IA e robôs, existindo também jogos como o aclamado *Detroit Become Human*[20], a qual narra a história dos robôs que buscam os seus lugares na sociedade, a fim de serem tratados com direitos e obrigações, como os humanos.

[16]https://rockcontent.com/blog/inteligencia-artificial/.
[17]https://www.salesforce.com/br/products/einstein/ai-deep-dive/.
[18]*Black Mirror* é uma série de televisão britânica antológica de ficção científica criada por Charlie Brooker e centrada em temas obscuros e satíricos que examinam a sociedade moderna, particularmente a respeito das consequências imprevistas das novas tecnologias. - https://pt.wikipedia.org/wiki/Black_Mirror.
[19]Episódio número três da quarta temporada, lançado em 29 de dezembro de 2017.
[20]Detroit: Become Human é um jogo eletrônico produzido pela Quantic Dream e publicado pela Sony Interactive Entertainment para o PlayStation 4 e Microsoft Windows PC. A história gira em torno de Kara, Markus e Connor, três androides concebidos pela empresa fictícia CyberLife que, consoante as decisões que o tomar, mudarão o rumo da cidade de Detroit e, consequentemente, dos Estados Unidos da América. Além disso, será testemunhado o surgimento de uma nova raça: Os Divergentes (androides que manifestam emoções humanas). - https://pt.wikipedia.org/wiki/Detroit:_Become_Human.

Contudo, fugindo da ficção e voltando a realidade, é fato que existem diversas tecnologias as quais muitas vezes nem são conhecidas pelas pessoas, um exemplo seria um programa da NVIDIA[21] referente às máquinas autônomas, onde em seu próprio site citam que "Os robôs da atualidade conseguem fazer muito mais do que só tarefas. Podem aprender, se adaptar e evoluir usando recursos como *machine learning*, visão computacional, navegação e muitos outros. Os sistemas NVIDIA® Jetson AGX™ usam o poder de *deep learning* para adentrar essa nova era da robótica inteligente integrada, desde a manufatura e a agricultura até a segurança e a assistência médica domiciliar."[22].

Destaca-se a parte que os sistemas da NVIDIA usam o poder de *deep learning* para as áreas de manufatura, agricultura, segurança e assistência médica domiciliar. Se for observado e analisado essa frase, pode surgir um grande e polêmico debate em torno disso, qual o manuseio de robôs na área de segurança e assistência médica hospitalar, pois, quem garante que uma máquina seja totalmente livre de erros inesperados e que elas não irão causar danos para algum paciente frágil internado em um hospital, por exemplo. Debate esse que remete a responsabilidade, próximo assunto que será abordado.

4 A RESPONSABILIDADE CIVIL NO DIREITO BRASILEIRO E NA UNIÃO EUROPEIA

Antes de adentrar especificamente no tema da IA e a responsabilidade dos danos causados por essa, é importante que se tenha uma breve concepção do que é entendido como responsabilidade na área do Direito Civil Brasileiro.

Para Carlos Roberto Gonçalves, a responsabilidade "tem sua origem na raiz latina *spondeo*, pela qual se vinculava o devedor, solenemente, nos contratos verbais do direito romano" e que "toda atividade que acarreta prejuízo traz em seu bojo, como fato social, o

[21]Nvidia Corporation (mais comumente referida como Nvidia, estilizada como NVIDIA ou, devido ao seu logotipo, nVIDIA) é uma empresa multinacional de tecnologia incorporada em Delaware e com sede em Santa Clara, Califórnia. Ela projeta unidades de processamentos gráficos (GPUs) para os mercados de jogos e profissionais, bem como o sistema em unidades de chip (SoCs) para o mercado de computação móvel e automotivo. - https://pt.wikipedia.org/wiki/Nvidia.

[22] https://www.nvidia.com/pt-br/autonomous-machines/robotics/.

problema da responsabilidade. Destina-se ela a restaurar o equilíbrio moral e patrimonial provocado pelo autor do dano."[23].

Importante também citar a diferença entre a responsabilidade objetiva e a subjetiva, sendo essa primeira a reparação de um dano em que exista culpa ou não, já a segunda se trata da responsabilidade quando existe culpa por parte do agente. Dessa forma, tem-se uma breve ideia do que se trata a responsabilidade.

Já a responsabilidade na área digital brasileiro ainda é muito recente, surgindo uma lei que o regula apenas em 2018, a Lei Geral de Proteção de Dados Pessoais, a qual traz em seu artigo 44 e incisos[24], as hipóteses de irregularidade do tratamento de dados, que se esse for irregular, haverá responsabilidade quanto à reparação de dados se forem causados pelo controlador, operador ou outro terceiro[25].

No caso, o artigo 44, da LGPD, traz a responsabilidade dos danos que foram causados decorrentes da violação de segurança de dados, contudo, ao analisar a Inteligência Artificial, vê-se que as possibilidades são infinitas e que não são apenas relacionadas a vazamento de dados, por exemplo. Portanto, como antes mencionado, o tema ainda é muito recente no Brasil, sendo necessário buscar paradigmas na legislação Europeia.

4.1 Responsabilidade dos robôs na União Europeia

Como foi exposto, o assunto ainda é muito recente no Brasil, logo a jurisprudência, doutrina e lei é muito restrita ao abordar sobre, fazendo necessário buscar respaldo na legislação Europeia. Um exemplo de destaque é a Diretiva do Parlamento Europeu (Diretiva 2010/40/EU)[26], que "estabelece um quadro para a implantação de sistemas de transporte inteligentes no transporte rodoviário, inclusive nas interfaces com outros modos de transporte",

[23]Direito civil brasileiro, volume 4: responsabilidade civil / Carlos Roberto Gonçalves. — 7. ed. — São Paulo: Saraiva, 2012.

[24]Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:
I - o modo pelo qual é realizado;
II - o resultado e os riscos que razoavelmente dele se esperam;
III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.
Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

[25]https://www.plugar.com.br/o-que-diz-a-lgpd-sobre-reparacao-de-danos/, bem como o artigo "A Responsabilidade Civil Dos Agentes De Tratamento De Dados E O Fato De Serviço Consumerista, Luca d'Arce Giannotti, Faculdade de Direito da Universidade de São Paulo, 2019.

[26] Diretiva 2010/40/UE Do Parlamento Europeu E Do Conselho de 7 de Julho de 2010.

expôs em seu artigo 11[27], que a responsabilidade será equivalente a Diretiva 85/374/CEE, ou seja, é comparado aos produtos defeituosos. Logo, se houver algum tipo de vazamento de dados, por exemplo, a União Europeia decidiu que o responsável será o fornecedor do serviço em que houve a falha (aludindo, de certa forma, ao Código de Consumidor).

Após o ano de 2010, outro exemplo sobre o tema e que remete a uma discussão polêmica aconteceu em fevereiro de 2017, onde o Parlamento Europeu editou a Resolução 2015/2103 (INL)[28], a qual trouxe certos limites, ou melhor dizendo, o legislador impôs alguns princípios éticos fundamentais que necessitam ser respeitados na hora de desenvolver, na programação e na utilização de máquinas que possuem inteligência artificial (robôs), a fim de evitar o máximo possível de danos[29].

A Resolução de 2017 trouxe também um rol que os "robôs teriam que seguir" para ser considerados autônomos, quais sejam: aquisição de autonomia através de sensores e/ou da trocade dados com o seu ambiente (interconectividade) e da troca de análise desses dados; autoaprendizagem com a experiencia e com a interação (critério opcional); um suporte mínimo; adaptação do seu comportamento e das suas ações no ambiente e a inexistência de vida no sentido biológico do termo[30].

[27]Artigo 11.o Regras relativas à responsabilidade Os Estados-Membros asseguram que as questões relativas à responsabilidade, quanto à implantação e à utilização de aplicações e serviços STI constantes das especificações aprovadas nos termos do artigo 6.o, sejam tratadas em conformidade com a legislação em vigor da União, nomeadamente a Directiva 85/374/CEE do Conselho, de 25 de Julho de 1985, relativa à aproximação das disposições legislativas, regulamentares e administrativas dos Estados-Membros em matéria de responsabilidade decorrente dos produtos defeituosos (1), bem como com a legislação nacional aplicável.

[28]https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_PT.html.

[29]Resolução 2015/2103 (INL), alínea B: "Considerando que, agora que a humanidade se encontra no limiar de uma era em que robôs, «bots», androides e outras manifestações de inteligência artificial (IA), cada vez mais sofisticadas, parecem estar preparados para desencadear uma nova revolução industrial, que provavelmente não deixará nenhuma camada da sociedade intacta, é extremamente importante que o legislador pondere as suas implicações e os seus efeitos a nível jurídico e ético, sem pôr entraves à inovação."

Alínea Z: "Considerando que, graças aos impressionantes avanços tecnológicos da última década, não só os robôs de hoje conseguem efetuar atividades que, regra geral, costumavam ser exclusivamente realizadas por humanos, como também o desenvolvimento de certas características autónomas e cognitivas – por exemplo, a capacidade de aprender com a experiência e de tomar decisões quase independentes – os tornaram cada vez mais similares a agentes que interagem com o seu ambiente e conseguem alterá-lo de forma significativa; considerando que, nesse contexto, a responsabilidade jurídica decorrente de uma ação lesiva de um robô constitui uma questão crucial."

13. "Destaca que o quadro ético orientador deve basear-se nos princípios de beneficência, não-maleficência, autonomia e justiça, nos princípios e valores consagrados no artigo 2.º do Tratado da União Europeia e na Carta dos Direitos Fundamentais, tais como a dignidade do ser humano, a igualdade, a justiça e a equidade, a não discriminação, o consentimento esclarecido, o respeito pela vida privada e familiar e a proteção de dados, bem como em outros princípios e valores subjacentes do direito da União, como a não estigmatização, a transparência, a autonomia, a responsabilidade individual e a responsabilidade social, e em códigos e práticas éticas existente."

[30]Princípios gerais relativos ao desenvolvimento da robótica e da IA para utilização civil, linha 1 - https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_PT.html.

Diante desse rol trazido pela edição da Resolução 2015/2103, surge a ideia de que algum dia a IA autônoma sairá da ficção e se tornará real por completo, e que, se essa se tornar realmente independente de qualquer comando, teria como consequência a sua responsabilização por seus atos. Nesse sentido, uma das soluções seria a atribuição da personalidade jurídica à Inteligência Artificial (assunto que ainda será abordado).

Para tanto, antes de analisar a responsabilidade dos atos autônomos da IA, bem como o nexo de causalidade, é importante pontuar primeiro sobre quais seriam esses atos e suas consequências, partindo ao próximo tema.

5 ATOS AUTÔNOMOS DA INTELIGÊNCIA ARTIFICIAL

Embora a Inteligência Artificial, o *machine learning* e o *deep learning* serem os responsáveis por facilitar o dia a dia das pessoas e tornarem suas atividades rotineiras mais simples, quando as máquinas adotam um certo conhecimento e se tornam então robôs com autoaprendizagem, é fato que em alguns momentos seus atos poderão ser independentes de um comando humano, por exemplo, (essa imprevisibilidade foi trazida em questão na Resolução de 2017, bem como a falta de um regulamento jurídico sobre os atos autônomos das máquinas inteligentes).

Ocorre que, sendo possível um robô com autoaprendizagem agir por conta própria, surge a questão de qual seria o limite de seus atos e quais seriam esses? Logo, a IA carrega como principal característica a interação dessas máquinas com o ambiente em que vivem, porém, quanto mais independentes esses sistemas são, mais difícil será de controlá-los, resultando na imprevisibilidade dos mesmos.

A partir dessa imprevisibilidade existente nas máquinas inteligentes e existindo algum dano indenizável[31], é necessário atribuir a algo ou alguém a responsabilidade do ato ilícito.

Contudo, como deve ser feita essa imposição da responsabilidade em caso, por exemplo, de um veículo autônomo32 que atropela um cidadão?

[31]Se observado a luz do Código Civil Brasileiro, se existe um ato ilícito que causou prejuízo a outrem, deve esseser indenizado, nos termos do artigo 186 e 927, do Código Civil.
Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.
Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.

Ainda sobre o exemplo do veículo autônomo, é necessário analisar o cenário do caso, como se a falha no sistema da máquina surgiu de um erro por um sistema autônomo defeituoso ou não, e ainda nesse sentido, de quem seria a culpa por tal erro existente? Diante disso, a necessidade do estudo do nexo causal é de extrema relevância ao responsabilizar alguém ou algo.

5.1 Nexo de Causalidade

Antes de aprofundar no tema, importante conceituar o nexo causal, sendo ele o vínculo existente entre a conduta do agente e o resultado por ela produzido[33],e, segundo Carlos Roberto Gonçalves: "Um dos pressupostos da responsabilidade civil é a existência de um nexo causal entre o fato ilícito e o dano produzido. Sem essa relação de causalidade não se admite a obrigação de indenizar. O art. 186 do Código Civil a exige expressamente, ao atribuir a obrigação de reparar o dano àquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem."[34].

Assim, para esclarecer sobre o assunto, imagine-se um imóvel particular que detém um sistema contra incêndios, onde se o detector de fumaças perceber algum indicio de fogo, liga automaticamente aos bombeiros mais próximos e os alertam, interrompendo também o fornecimento do gás e impedindo que portas e janelas se fechem para circular o ar. Porém, por algum motivo o sistema não funciona e os proprietários do imóvel são imensamente prejudicados, pois os bombeiros não foram alertados, por exemplo[35].

Surge então a questão de quem seria a responsabilidade por tal erro? Partindo do início, seria o desenvolvedor do sistema? O fornecedor do sistema? O usuário ou a provedora de internet que por um lapso interrompeu o fornecimento do serviço ao imóvel?

Diante do problema exemplificado, vê-se a importância de estudar o caso por completo a fim de descobrir onde foi o erro, para que então surja o responsável pelo mesmo. Importante também, mencionar que é possível que se aplique a exclusão da responsabilidade, como será posto a seguinte.

---

[32]Tal exemplo remete a história narrada anteriormente na passagem do episodio de *Black Mirror*, onde um veículo autônomo atropela um pedestre, lhe causando ferimentos e surgindo a dúvida de quem seria o responsável pelo fato.

[33]https://www.jusbrasil.com.br/topicos/291656/nexocausal#:~:text=%C3%89%20o%20v%C3%ADnculo%20existente%20entre,ao%20resultado%20previsto%20em%20lei.

[34] Direito civil brasileiro, volume 4: responsabilidade civil / Carlos Roberto Gonçalves. 7. ed. São Paulo:Saraiva, 2012.

[35] Exemplo retirado da revista escrita por ANTUNES, Henrique Sousa. Inteligência artificial e responsabilidade civil: enquadramento.Revista de Direito da Responsabilidade, ano 1, 2019.

5.2 Hipótese de Exclusão da Responsabilidade

Dá-se o nome de risco de desenvolvimento à hipótese de exclusão de responsabilidade quando, exemplificando, um desenvolvedor do *software* "A" adota a tecnologia mais avançada existente à época em que foi feito, mas que ao longo do tempo surge algum erro do programa desenvolvido "A", porém, mesmo se houver outro programa mais sofisticado e seguro "B", o desenvolvedor do *software* "A" não será responsabilizado, pois as tecnologias utilizadas eram as melhoras no momento.

Assim, se ocorrer algum dano indenizável e imprevisível que tenha conexão ao programa de *software*, o seu desenvolvedor não será responsabilizado pelos prejuízos, como antes mencionado, configurando então o risco do desenvolvimento[36].

6 PROVÁVEIS SOLUÇÕES A IMPUTAÇÃO DA RESPONSABILIDADE

Ao ocorrer um ato ilícito e configurado o liame causal entre a conduta do robô (vê-se também máquinas, *softwares*) e os danos que foram causados à vítima, deve ocorrer a imputação da responsabilidade a alguém ou algo. Como já exemplificado anteriormente, é imprescindível a análise do nível de intervenção de cada sujeito no caso, assim sendo, a

responsabilidade pode decair sobre: o desenvolvedor do programa; o fornecedor do programa; o usuário ou outro terceiro.

O problema da Inteligência Artificial e a responsabilidade ainda é muito recente, logo, são poucas hipóteses para resolver tal questão. Contudo, existem três hipóteses fortes para uma possível resolução do debate, sendo elas: a teoria do deep-pocket[37]; do seguro e da personalização jurídica dos robôs.

Entende-se como deep-pocket quando qualquer indivíduo envolvido em atos de riscos, mas sendo elas lucrativas e de utilidade para a sociedade, devem reembolsar os danos causados pelo lucro recebido[38]. Assim, o sujeito pode ser o desenvolvedor da inteligência (IA) ou o fabricante do produto, podendo ser a empresa ou o profissional que a utiliza em seu trabalho,

impondo a eles um seguro obrigatório o qual irá ressarcir os danos causados aos terceiros.

[36]Exemplo retirado do Artigo Científico de TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. Desafios da inteligência artificial em matéria de responsabilidade civil. Revista Brasileira de Direito Civil – RBD Civil, Belo Horizonte, v. 21, p. 61-86, jul./set. 2019.
[37]Em tradução livre, se tem "bolso profundo".

Nesse sentido, a Resolução 2015/2103 (INL) editada em 16 de fevereiro de 2017, trouxe em sua linha de número 57[38] uma possível solução no âmbito da União Europeia, sendo essa o regime de seguros obrigatórios (o qual já acontecia com os carros) que cobrem os atos robóticos, responsabilizando-os[39].

Logo, a terceira hipótese para a solução da imputação da responsabilidade, seria a personificação dos robôs, ou seja, torna-los pessoas jurídicas com direitos e deveres. Importante então, conceituar o termo "personalidade jurídica" como "a aptidão genérica para adquirir direito subjetivo, e é reconhecida a todo o ser humano independente da consciência ou vontade do indivíduo, esta é, portanto, um atributo inseparável da pessoa"[40].

O Secretariado da UNCITRAL[41] divulgou uma nota explicativa referente ao artigo 12[42]da Convenção das Nações Unidas sobre a Utilização de Comunicações Eletrônicas em Contratos Internacionais, onde esse estabelece o princípio de que a pessoa (sendo ela natural ou jurídica) necessita se responsabilizar por qualquer mensagem gerada pela máquina, ou seja, a disposição não reconhece a personalidade jurídica da IA pelas suas manifestações, mas sim à pessoa que agiu em nome da IA[43].

[38]PIRES, Thatiane Cristina Fontão; SILVA, Rafael Peteffi da. A responsabilidade civil pelos atos autônomos da inteligência artificial: notas iniciais sobre a resolução do Parlamento Europeu. *Rev. Bras. Polít. Públicas*, Brasília, v. 7, nº 3, p. 238-254, 2017.

[39]57. Destaca que uma possível solução para a complexidade de atribuir responsabilidade pelos danos causados pelos robôs cada vez mais autónomos pode ser um regime de seguros obrigatórios, conforme acontece já, por exemplo, com os carros; observa, no entanto que, ao contrário do que acontece com o regime de seguros para a circulação rodoviária, em que os seguros cobrem os atos e as falhas humanas, um regime de seguros para a robótica deveria ter em conta todos os elementos potenciais da cadeia de responsabilidade - https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_PT.html.

[40]"Maria Helena Diniz acentua que os direitos da personalidade são absolutos, intransmissíveis, indisponíveis, irrenunciáveis, ilimitados, imprescritíveis, impenhoráveis. Toda pessoa natural é sujeito de direito, portanto, é capaz de adquirir direitos e deveres na ordem civil" - https://jus.com.br/artigos/61828/a-personalidade-juridica- no-direito-civil.Nesse sentido, o artigo 1º, do Código Civil expõe que: Art. 1º Toda pessoa é capaz de direitos e deveres na ordemcivil.

[41]Traduzindo, A Comissão das Nações Unidas para o Direito do Comércio Internacional é um órgão subsidiário da Assembleia Geral da ONU responsável por ajudar a facilitar o comércio e o investimento internacional. - https://en.wikipedia.org/wiki/United_Nations_Commission_on_International_Trade_Law.

[42]Artigo 12. Uso de sistemas automatizados de mensagens na formação de contratos Um contrato formado pela interação entre um sistema automatizado de mensagens e uma pessoa natural, ou pela interação entre sistemas automatizados de mensagens, não deverá ser considerado inválido ou inexequível pelo simples fato de que nenhuma pessoa natural reviu ou interveio em cada uma das ações individuais efetuadas pelo sistema automatizadode mensagens ou o contrato resultante.

[43]Exemplo retirado do Artigo Cientifico PIRES, Thatiane Cristina Fontão; SILVA, Rafael Peteffi da. A responsabilidade civil pelos atos autônomos da inteligência artificial: notas iniciais sobre a resolução do Parlamento Europeu. Rev. Bras. Polít. Públicas, Brasília, v. 7, nº 3, 2017 p. 238-254.

Mesmo existindo alguns projetos legislativos que contrariam a hipótese de personalização jurídica da IA, como o de cima citado, ainda assim a hipótese é relevante para uma tentativa de solucionar o debate.

Nesse sentido, se a Inteligência Artificial independente de qualquer comando prévio, agindo então "por conta própria", pode-se imaginar que o robô tem certa consciência de seus atos e devendo então ser responsabilizado por esses. Se, portanto, for atribuída a personalidade jurídica às máquinas, deve-se então modificar totalmente o entendimento jurídico e adaptá-lo para que surjam normas que regulem a tal nova personalidade.[44]

E, portanto, se os robôs forem sujeitos de direitos e obrigações, esses poderiam ser responsáveis para indenizar qualquer dano causado por eles. Contudo, se pensar dessa maneira, poderiam eles serem punidos além de civilmente dizendo, mas também penalmente? Como seriam essas punições penais, os robôs seriam presos em alguma penitenciária robótica ou apenas desligados e descartador em um ferro-velho? Importante ressaltar que quando se fala em sanções ou punições, têm como objetivo despertar um sentimento de reprovação aos atos praticados, logo, um robô poderia ter esse sentimento de reprovação?

Curioso analisar que em outubro de 2017, o rei saudita, Salman bin Abdelaziz, concedeu pela primeira vez a cidadania a Sophia, um robô humanoide criado por uma empresa de Hong Kong chamada Hanson Robotics. Isso significa que, se a Sophia quisesse, ela poderia alugar

um apartamento nos arredores de Meca[45]. Contudo, o assunto teve alta relevância na Arábia Saudita, pois se trata de um país que sequer permitem que as mulheres podiam dirigir e ainda precisam de autorização do homem para muitas coisas[46].

Mesmo existindo o caso da Sophia (podendo ser considerado como uma exceção), o entendimento majoritário que se tem ao falar sobre personalidade jurídica aos robôs é que esse assunto, por hora, não é viável e seria uma saída de difícil acesso, pois seria necessário alterar todo o ordenamento jurídico existente para que fosse possível encaixar tal entendimento.

[44]Responsabilidade Civil e Inteligência artificial: Quem responde pelos danos causados por robôs inteligentes? Christine Albiani.
[45]https://www.gazetadopovo.com.br/economia/nova-economia/arabia-saudita-da-cidadania-a-um-robo-e-reacende-debate-sobre-direitos-e-deveres-de-maquinas-inteligentes-6cs0lnndez9axx3o7jvspbjnw/.
[46]https://www.uol.com.br/tilt/noticias/redacao/2018/07/08/robos-devem-ter-direitos-humanos.htm.

Dessa forma, o que prevalece é o entendimento das Nações Unidas sobre a Utilização de Comunicações Eletrônicas em Contratos Internacionais, por exemplo, a qual confere a responsabilidade a quem está por trás da máquina inteligente que agiu, sendo essa pessoa física ou jurídica, respondendo então objetivamente pelos danos causados[47]

Diante de uma sociedade que se vê cada vez mais utilizando tecnologias e que essas estão avançando de uma forma muito rápida, é fato que a questão sobre a responsabilidade deve ocorrer em um futuro próximo, podendo até mesmo ser resolvido o debate sobre a personalização jurídica da Inteligência Artificial. Certo é que as vítimas dos danos causados pelas máquinas autônomas não ficarão sem receber as devidas indenizações.

As opções referente ao *deep-pocket* ou ao seguro são os mais plausíveis e possíveis na atual sociedade, pois não haveria a importância de criar uma legislação totalmente nova e que mude por completo as leis atuais, logo, seria necessário apenas que os sujeitos mais afortunados (no caso do *deep-pocket*) sejam responsabilizados, ou, mesmo que não sejam detentores de fortunas, a ideia da criação de um seguro não é impossível e poderia resolver por completo as indenizações.

Já se a hipótese da personalização jurídica for utilizada, seria necessário a análise do grau de autonomia das máquinas e ainda deverá ser impostas penalidades para as práticas das

condutas ilícitas, entrando novamente na questão já abordada sobre o que seria uma penalidadepara um robô, o seu desligamento apenas iria resultar em um sentimento de reprovação à alguémque é feito de códigos, algoritmos, *softwares*, placas-mãe, etc.?

De qualquer forma, se for instituído ou não a personalidade jurídica às máquinas, o seguro ainda assim seria obrigatório, pois em todas as hipóteses deve existir um fundo de garantia que possa indenizar as vítimas dos atos ilícitos decorrentes das máquinas autônomas. Logo, esse projeto não traz uma solução para a discussão, mas sim as hipóteses existentes e quais as mais possíveis de se tornarem real, diante de que o assunto abordado ainda é muito recente principalmente no Brasil.

---

[47]Pode-se relacionar ao artigo 932, do Código Civil Brasileiro, o qual traz os responsáveis pelos atos de terceiros,nos seguintes termos:
Art. 932. São também responsáveis pela reparação civil:
I - os pais, pelos filhos menores que estiverem sob sua autoridade e em sua companhia;
II - o tutor e o curador, pelos pupilos e curatelados, que se acharem nas mesmas condições;
III - o empregador ou comitente, por seus empregados, serviçais e prepostos, no exercício do trabalho que lhes competir, ou em razão dele;
IV - os donos de hotéis, hospedarias, casas ou estabelecimentos onde se albergue por dinheiro, mesmo para fins de educação, pelos seus hóspedes, moradores e educandos;
V - os que gratuitamente houverem participado nos produtos do crime, até a concorrente quantia.

7 CONCLUSÕES

Está claro que a tecnologia apenas tende a avançar e como foi visto brevemente, a sua evolução se deu em um período muito rápido, pois em curto tempo se teve muito avanço e tecnologias que não eram esperadas. Então, com o surgimento da Inteligência Artificial, vê-se que o mundo tecnológico e moderno é ilimitado, e, consequentemente a IA também.

Hoje em dia, a IA age de forma autônoma, armazenando inúmeros dados com a *big data*e os processando por meio de *machine learning* e *deep learning* o que faz com que esses programas atuem cada vez mais independentes, ou seja, sem o mínimo ou nenhum comando de um humano. Consequentemente, podem existir falhas nesses atos, sendo eles por erro no programa ou não, ocasionando em atos ilícitos que trazem danos a terceiros, surgindo então o dever de indenizar.

Como foi visto no trabalho, o assunto abordado ainda é muito recente no Brasil, contudo,a União Europeia já prevê algumas soluções para o debate, como a imposição de alguns princípios éticos ao desenvolver *softwares* a fim de minimizar ao máximo os prejuízos que poderão ocorrer, bem como já entendem que os sujeitos responsáveis objetivamente pelos danossão os que atuam por trás das máquinas e não elas propriamente ditas.

Assim, se existente o ato ilícito, não se pode deixar de analisar o liame entre a conduta do robô e o dano indenizável ocorrido (nexo causal), o que remete a análise também do nível de intervenção de cada sujeito, como a responsabilidade sendo do desenvolvedor do programa,

do fornecedor/fabricante, do usuário ou de outros terceiros (frisa-se a hipótese de exclusão da responsabilidade do desenvolvedor).

Após traçar toda uma linha entre o que é Inteligência Artificial, seus atos autônomos que podem gerar prejuízos a alguém e observando as responsabilidades por trás disso, chega- se às hipóteses de possíveis soluções a discussão de quem será o responsável. Trazendo então a teoria do *deep-pocket*, onde o sujeito com o "bolso profundo" deve indenizar a vítima, ou osfundos de garantia (seguros) que deveriam ser obrigatórios, e, por fim, a configuração da personalidade jurídica aos robôs

Como visto no trabalho, foi exposta diversas situações e hipóteses sobre a IA e seus atos autônomos, porém, o objetivo real do trabalho não é buscar uma solução para tal embate, mas sim expor ao leitor as possibilidades existentes no atual cenário e mostrando também o que se pode esperar de um futuro próximo, como o avanço cada vez maior da IA e a possibilidade desses um dia serem considerados pessoas com direitos e obrigações.

REFERÊNCIAS

ALBIANI, Christine. Responsabilidade Civil e Inteligência artificial: Quem responde pelos danos causados por robôs inteligentes? **Itsrio**. Disponível em: https://itsrio.org/wp-content/uploads/2019/03/Christine-Albiani.pdf. Acesso em: 03 de maio de 2020.

ANTUNES, Henrique Sousa. Inteligência artificial e responsabilidade civil: enquadramento. **Revista de Direito da Responsabilidade**, ano 1, 2019.

ASSED FERREIRA, Gustavo, COSTA POLI Luciana, SUSANA DE SOUSA GONÇALVES Anabela e SÓNIA MOREIRA DA SILVA, Eva. In: **VII Encontro Internacional Do Conpedi /Braga - Portugal Direito Civil Contemporâneo**, 2017. Disponível em: http://conpedi.danilolr.info/publicacoes/pi88duoz/c3e18e5u/7M14BT72Q86shvFL.pdf. Acesso em: 13 de jun. 2020.

BITTENCOURT GUARIENTO, Daniel; MAFFEIS MARTINS, Ricardo. Inteligência artificial e responsabilidade civil dos robôs. **Migalhas.** Disponível em: https://www.migalhas.com.br/coluna/impressoes-digitais/313834/inteligencia-artificial-e-responsabilidade-civil-dos-robos. Acesso em: 13 jun. 2020.

COELHO, Carlos. "Arábia Saudita dá cidadania a um robô e reacende debate sobre direitos e deveres de máquinas inteligentes". **Gazeta do Povo**. Disponível em: https://www.gazetadopovo.com.br/economia/nova-economia/arabia-saudita-da-cidadania-a-um-robo-e-reacende-debate-sobre-direitos-e-deveres-de-maquinas-inteligentes-6cs0lnndez9axx3o7jvspbjnw/. Acesso em: 28 jul. 2020.

D'ARCE GIANNOTTI, Luca. a responsabilidade civil dos agentes de tratamento de dadose o fato de serviço consumerista. **Faculdade de Direito da Universidade de São Paulo**, 2019. Disponível em: https://www.levysalomao.com.br/files/fckeditor/file/Monografia%202%20colocado.pdf. Acesso em: 27 jun. 2020.

DIRETIVA 2010/40/UE DO PARLAMENTO EUROPEU E DO CONSELHO DE 7 DE JULHO DE 2010. **Jornal Oficial da União Europeia**. Disponível em: https:// https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32010L0040&from=BG. Acesso em: 24 maio 2020.

ELECTRONIC NUMERICAL INTEGRATOR AND COMPUTER (ENIAC). **Wikiédia, a enciclopédia livre**. Disponível em: https://pt.wikipedia.org/wiki/ENIAC. Acesso em: 28 jun. 2020.

ÉPOCA NEGÓCIOS ONLINE. Leia o texto do convite que criou o termo inteligência artificial. Disponível em: https://epocanegocios.globo.com/Tecnologia/noticia/2019/03/leia-o-texto-do-convite-que-criou-o-termo-inteligencia-artificial.html. Acesso em: 28 jun. 2020.

GONÇALVES, Carlos Roberto. **Direito civil brasileiro:** responsabilidade civil. 7.ed. São Paulo, SP: Editora Saraiva, 2012. v. 4 . 561 p.

GRANATYR, Jones. Teste de Turing. **Iaexpert academy**. Disponível em:

https://iaexpert.academy/2016/07/19/historico-da-ia-teste-de-turing/. Acesso em: 27 jun. 2020.

LA PASCALINE. **Wikiédia, a enciclopédia livre.** Disponível em: https://pt.wikipedia.org/wiki/La_pascaline. Acesso em: 24 jun. 2020.

MOUTINHO, Célia. Gabinete do Património Histórico da Caixa Geral de Depósitos Setembrode 2011. **CGD.** Disponível em: https://www.cgd.pt/Institucional/Patrimonio-Historico-CGD/Estudos/Documents/Maquinas-de-escrever.pdf. Acesso em: 24 jun. 2020.

NUNES, Sérgio Sobral. Introdução aos Computadores. Computadores e Redes de Comunicação Mestrado em Gestão de Informação. **FEUP 06/07**. Disponível em: https://web.fe.up.pt/~ssn/disciplinas/crc/computadores.pdf. Acesso em: 24 jun. 2020.

PARLAMENTO EUROPEU. Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica (2015/2103(INL)). Disponível em::https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_PT.html. Acesso em: 24 maio 2020.

PIRES, Thatiane Cristina Fontão; SILVA, Rafael Peteffi da. A responsabilidade civil pelos atos autônomos da inteligência artificial: notas iniciais sobre a resolução do Parlamento Europeu. **Rev. Bras. Polít. Públicas**, Brasília, v. 7, n. 3, p. 238-254, 2017. Disponível em: ɬhttps://www.publicacoesacademicas.uniceub.br/RBPP/article/download/4951/3643. Acesso em: 13 jun. 2020.

RUSSELL, Stuart J. (Stuart Jonathan), 1962. **Inteligência artificial**. Stuart Russell, Peter Norvig; tradução Regina Célia Simille. Rio de Janeiro: Elsevier, 2013.

SARAIVA, Márcio. Um "exame de DNA" na carreira de dois grandes cientistas para descobrirmos o "pai" da nossa profissão. **UFCG.** Disponível em: http://www.dsc.ufcg.edu.br/~pet/jornal/agosto2009/materias/carreira.html. Acesso em: 24 jun. 2020.

TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. Desafios da inteligência artificial em matériade responsabilidade civil. **Revista Brasileira de Direito Civil – RBD Civil**, Belo Horizonte, v. 21, p. 61-86, jul./set. 2019. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/download/465/308. Acesso em: 13 jun. 2020.

WHITBY, Blay. **Inteligência artificial**: um guia para iniciantes; tradução de Cláudio Blanc. São Paulo: Madras, 2004.

A RESPONSABILIDADE CIVIL E A IMPORTÂNCIA DA REVISÃO HUMANA NAS DECISÕES AUTOMATIZADAS PREVISTAS NA LGPD.

LIABILITY AND THE IMPORTANCE OF HUMAN REVIEW IN AUTOMATED DECISIONS FORESEEN IN THE LGPD.

JÚLIA MENDES DE SOUZA[1]

SUMÁRIO: 1. INTRODUÇÃO. 2. CONCEITO DE INTELIGÊNCIA ARTIFICIAL (IA) E SEU FUNCIONAMENTO. 2.1. Responsabilidade Civil. 3. AS DECISÕES AUTOMATIZADAS E A REGULAMENTAÇÃO DADA PELA LGPD. 4. TEORIAS SOBRE A RESPONSABILIDADE CIVIL DE MÁQUINAS INTELIGENTES. 5. A RESPONSABILIDADE CIVIL PELAS DECISÕES AUTOMATIZADAS E A NECESSIDADE DE REVISÕES REALIZADAS POR PESSOA NATURAL. 6. PROPOSIÇÕES CONCLUSIVAS. REFERÊNCIAS BIBLIOGRÁFICAS**.**

RESUMO

O presente artigo busca trazer uma análise sobre a responsabilidade civil e as decisões automatizadas, tomadas por máquinas artificialmente inteligentes, e a importância da possibilidade de revisão humana, que foi retirada da atual redação do artigo 20 da lei em referência.

Palavras-chave: Lei Geral de Proteção de Dados; Responsabilidade civil; Inteligência artificial.

ABSTRACT

The present article seeks to bring an analysis of civil liability and automated decisions, made by artificially intelligent machines, and the importance of the possibility of human review, which was removed from the current wording of Article 20 of the law in reference.

Keywords: General Data Protection Law; Liability; Artificial Intelligence.

1. INTRODUÇÃO

A utilização da Inteligência Artificial (IA), bem como a da Internet das Coisas (IOT), já é presente na rotina da maior parte das pessoas. As tecnologias se renovam diariamente, sempre surge uma nova versão de algum objeto, e cada vez essas versões se tornam mais inteligentes.

[1]Estudante do 4º ano diurno do curso de graduação em Direito na Faculdade de Direito de Sorocaba, e integrante do Grupo de Pesquisa em Direito Digital do ano de 2020, da Instituição.

Entretanto, observa-se que a regulamentação para o uso dessas ferramentas não se reproduz com a mesma velocidade, de modo que o ordenamento jurídico já existente se torna insuficiente, ou, até mesmo, obsoleto.

No cenário internacional, sobretudo europeu, já existe legislação específica (GDPR - *General Data Protection Regulation*[2]), além de diversas discussões sobre a repercussão das decisões tomadas pelos equipamentos dotados de inteligência artificial em relação ao cenário jurídico. O Brasil, porém, encontra-se demasiadamente atrasado, visto que as inovações tecnológicas não se estagnam, havendo necessidade de regulamentação há muito tempo. Nesse campo, surge a recente Lei Geral de Proteção de Dados, que busca regrar o tratamento de dados, bem como as decisões automatizadas.

Sobre o tema, um aspecto de extrema relevância é o da responsabilidade civil, uma vez que, em diversas áreas, muitas escolhas já não são mais realizadas por pessoas naturais, de modo que se torna duvidoso a quem incumbe o dever de indenizar possíveis danos causados por tal deliberação. Ainda que a atuação das máquinas diminua as chances de ocorrerem eventos danosos, não há garantia de que estes não venham, em hipótese alguma, a acontecer. É o que se busca debater no presente artigo, sem, contudo, esgotar o assunto.

2 CONCEITO DE INTELIGÊNCIA ARTIFICIAL (IA) E SEU FUNCIONAMENTO

Como dito anteriormente, a Inteligência Artificial marca presença na rotina da maior parte da população mundial. Então, antes de adentrar na discussão jurídica propriamente dita, mostra-se necessária uma introdução conceitual, inicialmente da inteligência humana, para que seja possível compreender a relação com a inteligência presente nos equipamentos artificialmente inteligentes.

Segundo o Dicionário Michaelis On-line, a inteligência é definida como uma faculdade de entender, pensar, raciocinar e interpretar, isto é, entendimento, intelecto, percepção, inteligência: conjunto de funções mentais que facilitam o entendimento das coisas e dos fatos.[3] Pensando em uma forma de reproduzir a inteligência em uma máquina, a IA pode ser conceituada como a capacidade de um robô compreender, raciocinar, pensar e interpretar, de maneira similar à humana.

[2]Regulamento Geral de Proteção de Dados.

[3]INTELGIÊNCIA. In: MICHAELIS, Dicionário Brasileiro da Língua Portuguesa. São Paulo: Editora Melhoramentos, 2021. Disponível em: https://michaelis.uol.com.br/busca?r=0&f=0&t=0&palavra=intelig%C3%AAncia. Acesso em 29 nov. 2021.

O estudo sobre esse tema é antigo. Em 1930, Alan Turing, hoje considerado o pai da computação, criou um projeto de um computador e de inteligência artificial.[4] A máquina criada por Turing era capaz de manipular, automaticamente, símbolos em um sistema de regras próprias. Assim, desenvolveu-se um sistema capaz de processar códigos semelhantes aos que hoje são denominados códigos criptografados[5]. Foi dessa forma que Turing passou a integrar o escritório de decodificação de mensagens da Inteligência Britânica, auxiliando na derrota dos nazistas na Segunda Guerra Mundial, em 1945. Por isso, demais menções sobre a IA se iniciaram próximas da data do fim do mencionado conflito.

Outro registro interessante data de 1943, quando o neuroanatomista Warren McCulloch e o cientista cognitivo Walter Pitts propuseram um modelo de neurônio artificial.[6] A teoria propunha que cada neurônio executasse uma operação lógica básica, combinando múltiplas entradas em uma única saída binária: verdadeira ou falsa.[7]

Desde então, o assunto é amplamente discutido e debatido, com diversas modificações em relação ao passado, em testes e avanços na compreensão de como esses objetos funcionam. A forma pela qual as máquinas inteligentes operam ocorre por meio de redes neurais artificiais (RNA), que são "técnicas computacionais que apresentam um modelo matemático inspirado na estrutura neural de organismos inteligentes e que adquirem conhecimento através da experiência".[8]

Segundo o volume 2, da série de pesquisas da Escola Superior do Ministério Público da União:

> O aprendizado de máquina é um algoritmo que, em face de novos dados que são apresentados, calibra automaticamente os pesos da rede a fim de apresentar melhores resultados. Surden (2014) descreve que:

[4]YUGE, Claudio. *Há 65 anos morria Alan Turing, o "Pai da Computação" e da IA***.** 07 out. 2019. Disponível em: <https://www.tecmundo.com.br/ciencia/142291-ha-65-anos-morria-alan-turing-pai-computacao-daia.htm#:~:text=Ele%20sempre%20alimentou%20interesse%20por,de%20intelig%C3%AAncia%20artificial%20(IA). Acesso em: 07 nov. 2020.

[5]Criptografia é a prática de codificar e decodificar dados. Quando os dados são criptografados, é aplicado um algoritmo para codificá-los de modo que eles não tenham mais o formato original e, portanto, não possam ser lidos. KASPERSKY. O que é criptografia de dados? Definição e explicação. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/encryption. Acesso em 07 nov. 2020.

[6]MAGRANI, Eduardo. Máquina que pensa. 21 mar. 2018. Disponível em: http://eduardomagrani.com/maquina-que-pensa/. Acesso em: 19 jun. 2020.

[7]BRAINNIAC. O cérebro é um modelo útil para a Inteligência Artificial? 14 jun. 2020. Disponível em: http://www.brainniac.ufv.br/index.php/o-cerebro-e-um-modelo-util-para-a-inteligencia-artificial/. Acesso em: 22 jun. 2020.

[8]DE CARVALHO, André Ponce de Leon Ferreira. Redes Neurais Artificiais. Mar. 2009. Disponível em: https://sites.icmc.usp.br/andre/research/neural/#:~:text=Redes%20Neurais%20Artificiais%20s%C3%A3o%20t%C3%A9cnicas,adquirem%20conhecimento%20atrav%C3%A9s%20da%20experi%C3%AAncia.

> o significado de aprendizado no contexto de machine learning: é a habilidade de melhorar a performance por meio da detecção de novos e melhores padrões a partir de novos dados. [...] Um algoritmo de aprendizagem de máquina pode se tornar mais preciso na execução de uma tarefa (como classificar um e-mail como SPAM) ao longo do tempo, porque seu projeto permite que ele aperfeiçoe continuamente seu modelo interno por meio da análise de mais exemplos e inferência de padrões novos e úteis a partir desses dados adicionais. Essa habilidade de aperfeiçoar sua performance ao longo do tempo pela análise contínua de novos dados detectando novos padrões úteis é o atributo-chave que caracteriza o aprendizado de máquina. (SURDEN, 2014, p. 92)'
>
> O aprendizado de uma RNA ocorre pela mudança dos pesos sinápticos dos neurônios da rede, cujas alterações buscam melhorar o resultado ou o desempenho por ela apresentados. A ideia é buscar continuamente reforçar as conexões que otimizam os resultados, selecionando os padrões mais úteis para a tarefa que se quer executar, enquanto se enfraquecem as conexões que não estão associadas a bons resultados.[9]

Superado o conceito de redes neurais artificiais, resta esclarecer como as máquinas, dentro dessas redes, são capazes de aprender. Existem três formas principais: aprendizado supervisionado; aprendizado não supervisionado; e reforço de aprendizagem.

No primeiro modelo de aprendizagem (supervisionada), são inseridos dados de entrada (informações) e dados de saída (classificação da informação).[10] Por exemplo, suponha que uma máquina esteja sendo treinada para identificação de cachorros. Como dados de entrada, serão inseridas diversas fotos de cachorro rotuladas como "cachorro" e fotos de outros animais rotuladas como "isto não é um cachorro". Ao final, o robô reconhecerá como e o que é o animal rotulado, classificando as fotos como "isto é um cachorro", mas não saberá classificar animais que não sejam cachorros.

É exatamente isso que ocorre, citando outro exemplo, em algoritmos do *Google*, em que é solicitado que assinalemos as imagens que possuem a imagem de um carro. A partir desse ato, estamos rotulando as imagens, classificando as informações e, consequentemente, auxiliando no treinamento da máquina da empresa.

De outro lado, há o aprendizado não supervisionado, em que, diferentemente do aprendizado supervisionado, não existem dados de saída, apenas de entrada, de modo que a máquina classificará de forma autônoma as informações inseridas. Nesse caso, a consequência

[9]GUEDES, Marcelo Santiago; MACHADO, Henrique Felix de Souza. Veículos autônomos inteligentes e a responsabilidade civil nos acidentes de trânsito no Brasil. Volume 02. Brasília. ESMPU, 2020. p. 41-42. Disponível em: http://escola.mpu.mp.br/a-escola/comunicacao/noticias/esmpu-lanca-publicacao-sobre-responsabilidade-civil-nos-acidentes-com-veiculos-autonomos/veiculos-autonomos-inteligentes.pdf. Acesso em: 07 nov. 2020.

[10]BARROS, Pedro. Aprendizagem de Maquina: Supervisionada ou Não Supervisionada? 07 abr. 2016. Disponível em: https://medium.com/opensanca/aprendizagem-de-maquina-supervisionada-ou-n%C3%A3o-supervisionada-7d01f78cd80a. Acesso em: 19 jun. 2020.

será o agrupamento de informações semelhantes.[11] A partir de uma situação hipotética, suponha que são inseridas em um robô mil fotos de frutas, entre elas banana, maçã e morango. A resposta (dados de saída) que ele dará será o agrupamento das imagens semelhantes, ou seja, cada tipo de fruta formará um grupo. Isso já vem sendo utilizado em alguns lugares no campo de pesquisas, de modo que ao digitar, por exemplo, "LGPD e a inteligência artificial". O software buscará, dentre os vários artigos, o grupo que possui essas palavras, agrupando os artigos semelhantes.

O terceiro modo de aprendizagem que merece destaque é o reforço da aprendizagem. Trata-se de procedimento mais complexo, pois nessa situação a máquina aprende a realizar determinada tarefa em um sistema de tentativa e erros, conjuntamente a um sistema de recompensas.[12] Com isso, em um jogo digital, por exemplo, a máquina tem a capacidade de perceber que perde pontos (ou o jogo) realizando determinada ação, e fazendo outra (ação) ela adquire pontos (recompensa). Assim que ela "aprende" as regras do jogo, busca maximizar a recompensa total (pontos), de modo que se torna a melhor na tarefa que executa.

Ressalta-se, contudo, que prestar informações sobre o motivo pelo qual uma decisão foi tomada não é de natureza da IA, por isso ainda não se sabe com precisão como os robôs adquirem essa capacidade de aprender sozinhos. Da mesma forma, considerando que o algoritmo continua em aprendizagem durante o seu funcionamento, também não será possível voltar ao conjunto de regras iniciais, em relação ao começo do processo de aprendizagem da máquina.[13]

2.1 Responsabilidade civil

O termo "responsabilidade" traz consigo a ideia de reparação de prejuízos causados a outrem. Resumidamente, no âmbito do direito civil, aplicando-se a ideia supracitada, temos que, ao causar dano a outra pessoa, há o dever de indenizar, expresso no Código Civil de 2002

[11]BARROS, Pedro. Aprendizagem de Maquina: Supervisionada ou Não Supervisionada? 07 abr. 2016. Disponível em: https://medium.com/opensanca/aprendizagem-de-maquina-supervisionada-ou-n%C3%A3o-supervisionada-7d01f78cd80a. Acesso em: 19 jun. 2020.
[12]DATA SCIENCE ACADEMY. Deep Learning Book Brasil. In: DATA SCIENCE ACADEMY. Capítulo 62: O Que é Aprendizagem Por Reforço? Disponível em: http://deeplearningbook.com.br/o-que-e-aprendizagem-por-reforco/. Acesso em: 19 jun. 2020.
[13]GUEDES, Marcelo Santiago; MACHADO, Henrique Felix de Souza. Veículos autônomos inteligentes e a responsabilidade civil nos acidentes de trânsito no Brasil. Volume 02. Brasília. ESMPU, 2020. p. 47. Disponível em: http://escola.mpu.mp.br/a-escola/comunicacao/noticias/esmpu-lanca-publicacao-sobre-responsabilidade-civil-nos-acidentes-com-veiculos-autonomos/veiculos-autonomos-inteligentes.pdf. Acesso em: 07 nov. 2020.

em seu artigo 186: "Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito".

Do texto legal, extraem-se os requisitos legais para que haja o dever de reparação do dano: ação ou omissão; culpa ou dolo; dano; nexo de causalidade entre a ação ou omissão e o dano. Então, a primeira conclusão é: não haverá o dever de indenizar, se não houver dano ou se este não tiver relação (nexo de causalidade) com a ação ou omissão realizada.[14] No campo da omissão, a responsabilidade civil torna-se evidente quando há o dever legal de agir, ou seja, quando a lei impõe que se faça algo.

Aqui cabe uma distinção, pois a responsabilidade civil se divide em: responsabilidade civil subjetiva e objetiva. Na primeira, em síntese, é necessário que se prove a culpa ou dolo da ação praticada pelo sujeito, para que, então, haja dever de indenizar. Já a responsabilidade objetiva independe da prova de culpa ou dolo na ação praticada pelo sujeito para que haja dever de indenizar, bastando a prova de causalidade entre o dano e ação ou omissão.

A teoria que busca explicar a responsabilidade objetiva é chamada de "teoria do risco", e defende que qualquer sujeito que exerce atividade geradora de algum tipo de risco para terceiros, deve ser responsabilizado ainda que não tenha agido com dolo ou culpa, tendo obrigação de reparar o dano causado[15]. A teoria em referência é admitida pelo ordenamento jurídico brasileiro, em alguns casos, como a responsabilidade dos donos por seus animais, expressa no artigo 936 do Código Civil. O dono ou detentor do animal ressarcirá o dano por este causado, se não provar culpa da vítima ou força maior.

Com relação à responsabilidade do Estado, esta será objetiva quando o dano resultar de ação estatal, com direito de regresso ao agente que causou o prejuízo, conforme §6º do artigo 37 da Constituição Federal, e subjetiva quando o dano resultar de omissão.

Ainda no que diz respeito ao direito das obrigações, existe a figura jurídica da "obrigação solidária", isto é, o fenômeno jurídico em que há pluralidade de agentes, no polo passivo (devedores), no polo ativo (credores), ou em ambos, incorrendo sobre eles a obrigação pelo débito todo, ou direito pela prestação inteira, como se cada um fosse o único credor ou

[14] DANTAS, Aldemiro. Responsabilidade civil para leigos (brevíssima noção). Nov. 2013. Disponível em: : https://aldemirodantas.jusbrasil.com.br/artigos/121935826/responsabilidade-civil-para-leigos-brevissima-nocao#:~:text=Como%20se%20v%C3%AA%2C%20portanto%2C%20para,ou%20imprudente%20(com%20culpa). Acesso em: 20 jun. 2020.

[15]GONÇALVES, Carlos Roberto. *Direito Civil Brasileiro:* responsabilidade Civil. 14. Ed. São Paulo: Saraiva jur, 2019. Vol. 4.

devedor da obrigação.[16] Esta solidariedade não se presume e deve existir somente em função de lei ou contrato (artigo 265 do Código Civil), sendo regulamentada pelo Código Civil nos seguintes artigos: Art. 264. Há solidariedade, quando na mesma obrigação concorre mais de um credor, ou mais de um devedor, cada um com direito, ou obrigado, à dívida toda. Art. 265. A solidariedade não se presume; resulta da lei ou da vontade das partes.

A fim de tornar o conceito a um ponto mais concreto, passemos a um exemplo: A e B são devedores solidários de um empréstimo realizado com C, no valor de R$ 10.000,00 (dez mil reais). Havendo solidariedade entre os devedores, poderá o credor C cobrar a dívida em sua integralidade de qualquer um deles. Se B paga o valor total da dívida, terá direito de cobrar de A sua parte, isto é, R$ 5.000,00 (cinco mil reais), o que se denomina direito de regresso.

3 AS DECISÕES AUTOMATIZADAS E A REGULAMENTAÇÃO DADA PELA LGPD

Decisões automatizadas são aquelas tomadas por meios exclusivamente tecnológicos, ou seja, máquinas (robôs), com base em tratamento de dados[17] previamente realizado (vide formas de aprendizagem de máquinas – tópico 1).

Preliminarmente, a fim de que não restem dúvidas, o tratamento de dados está conceituado no artigo 5º, inciso X, da LGPD:

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

Superada a questão conceitual, passamos à análise do conteúdo normativo da lei. O artigo 20 da Lei Geral de Proteção de Dados, em sua primeira redação dispunha:

> Art. 20. O titular dos dados tem direito a solicitar revisão, por pessoa natural, de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive de decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

[16]DIAZ, Caroline Borota. *Responsabilidade Solidária no Direito Civil comparada ao Direito do Trabalho.* 2016. Disponível em: https://carolineborota.jusbrasil.com.br/artigos/437649443/responsabilidade-solidaria-no-direito-civil-comparada-ao-direito-do-trabalho#:~:text=Segundo%20o%20C%C3%B3digo%20Civil%20vigente,credor%20ou%20devedor%20da%20obriga%C3%A7%C3%A3o. Acesso em: 07 nov. 2020.

[17]Tratamento de dados: qualquer atividade que utilize dados pessoais.

Observa-se que o dispositivo em questão foi redigido consoante ao Regulamento Geral Europeu de Proteção de Dados: *General Data Protection Regulation,* popularmente conhecida como GDPR, cuja redação do artigo 22, *caput*, dispõe:

> 1. O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.[18]

O artigo 20, da LGPD, sofreu alterações e, atualmente, dispõe:

> Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (Redação dada pela Lei nº 13.853, de 2019) Vigência
> § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.
> § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

Observa-se que a obrigatoriedade de a revisão ser realizada por pessoa natural foi excluída. Dessa forma, a partir da análise dos parágrafos do dispositivo, para que se obtenha uma revisão de uma decisão tomada exclusivamente por meios tecnológicos, deverão ser solicitadas ao controlador[19] informações sobre os critérios observados pela máquina para que aquela decisão automatizada tenha sido tomada. Na hipótese de essas informações não serem fornecidas, poderá a ANPD[20] realizar uma auditoria a fim de que haja verificação se foram inseridos dados de entrada discriminatórios na máquina.

Nesses aspectos mencionados, no entanto, há uma observação a ser feita: como explicado anteriormente, há o tipo de aprendizagem em que a máquina adquire conhecimento sozinha, por meio de tentativa e erro, dentro de um sistema de recompensas (reforço de aprendizagem), procedimento este que ainda não é integralmente compreendido pela comunidade acadêmica. Em outras palavras, até pode haver informações sobre os critérios

[18]GALVÃO & SILVA ADVOCACIA. GDPR em português – Texto na Íntegra. Disponível em: https://www.galvaoesilva.com/lei-gdpr-em-portugues/. Acesso em: 20 jun. 2020.
[19]Artigo 5º, IV, LGPD: "VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais".
[20]Autoridade Nacional de Proteção de Dados – artigo 5º, XIX, LGPD: "XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional".

utilizados pela máquina, ou ser analisado se foi inserido algum tipo de preconceito para análise de dados, mas, na realidade, não será possível saber de forma inequívoca como a decisão automatizada foi tomada, daí a necessidade da revisão humana.

4 TEORIAS SOBRE A RESPONSABILIDADE CIVIL DE MÁQUINAS INTELIGENTES

Acerca da responsabilidade civil quanto às decisões automatizadas que causem danos às pessoas, existem algumas teorias: teoria norte-americana do *deep-pocket* (ou do bolso profundo); a teoria que defende um regime de seguros obrigatórios; e a teoria que defende a instituição obrigatória de um fundo de compensação.

A Teoria Norte-Americana do *deep-pocket* ou do bolso profundo, defende que as pessoas que realizam atividades de risco e lucrativas devem ser responsáveis por indenizar o dano, caso ele venha a ocorrer. Isso quer dizer que o desenvolvedor de produtos, softwares, inteligentes artificialmente e, portanto, capazes de tomar uma decisão sozinho, têm o "bolso profundo", pois aufere lucro, apesar de haver riscos inerentes à atividade explorada, e deve arcar com as consequências do dano. Nota-se que essa linha de pensamento se assemelha com a "teoria do risco", já utilizada pelo Código Civil em determinadas situações, como mencionado no tópico sobre responsabilidade civil objetiva.

A segunda teoria mencionada defende a imposição de um regime de seguros obrigatórios e já foi discutida pelo Parlamento Europeu.[21] O raciocínio utilizado pelos defensores dessa teoria é o de que, na possibilidade de o prejuízo ocorrer, o fornecedor responderá objetivamente, devendo antecipadamente "reservar" recursos para essa hipótese. Por isso, ao comprar um serviço ou produto que faça uso da inteligência artificial e que, em algum momento, poderá tomar uma decisão automatizada, deverá o comprador, conjuntamente à contratação, realizar um pacto de seguro que seja capaz de arcar financeiramente com as consequências do possível dano.

A terceira teoria mencionada é alternativa e ainda muito criticada ao defender a instituição obrigatória de um fundo de compensação. Segundo os defensores de tal corrente de pensamento, admite-se que os possíveis danos causados por robôs poderão ser ressarcidos a

[21]CNSeg. Parlamento Europeu cogita criar contratação compulsória de seguro de responsabilidade civil para inteligência artificial. 27 dez. 2017. Disponível em: https://cnseg.org.br/noticias/parlamento-europeu-cogita-criar-contratacao-compulsoria-de-seguro-de-responsabilidade-civil-para-inteligencia-artificial.html. Acesso em: 21 jun. 2020.

partir de um fundo de compensação alimentado pelas próprias máquinas. Nesse sentido, afirmam Ricardo Maffeis e Daniel Bittencourt Guariento:

> Melhor explicando, e traçando um paralelo entre a força de trabalho humana e a força de trabalho dos robôs – que, cada vez mais, agem de forma autônoma, raciocinando e tomando decisões, gerando lucro para seus "empregadores" e, portanto, fazendo jus a uma "remuneração" – os ganhos proporcionados pela "atividade laboral" destas "máquinas pensantes" reverteriam para o mencionado fundo de compensação.[22]

Existem vários pontos que merecem ser questionados. O principal deles é: se considerarmos que um robô exerce atividade laboral, tendo direito a uma remuneração, teríamos, também, que considerar que faz jus a outros direitos trabalhistas, como férias, 13º (décimo terceiro) salário, entre outros e, principalmente, considerar que a máquina possui personalidade jurídica (aptidão genérica para se adquirir direitos e deveres), equiparando-a a um verdadeiro cidadão.

Assim, analisando as três teorias em referência, nota-se que todas determinam a responsabilidade objetiva dos fabricantes por possíveis danos causados.

Ainda que seja questionado, na terceira teoria, em que a responsabilidade seria, em verdade, da máquina, temos que, ao se comparar a um trabalhador, como explicado pelos autores Ricardo Maffeis e Daniel Bittencourt Guariento, dever-se-ia, em tese, aplicar-se a responsabilidade objetiva, uma vez que as pessoas jurídicas respondem por danos causados por seus funcionários, conforme disposto no artigo 932, III, do Código Civil. Art. 932: "São também responsáveis pela reparação civil: III - o empregador ou comitente, por seus empregados, serviçais e prepostos, no exercício do trabalho que lhes competir, ou em razão dele;"

5 A RESPONSABILIDADE CIVIL PELAS DECISÕES AUTOMATIZADAS E A NECESSIDADE DE REVISÕES REALIZADAS POR PESSOA NATURAL

Dentre as teorias elencadas, analisando o atual Código Civil, e ponderando o cenário global contemporâneo, tem-se como a mais factível para responsabilidade civil de decisões automatizadas, a teoria norte-americana do *deep-pocket*, com as devidas ressalvas.

Em primeiro lugar, deve ser analisada a origem do erro no qual incorreu a máquina, ou seja, trata-se de um "defeito de fábrica", ou é decorrente do mau uso do programa? Na primeira

[22]MAFFEIS, Ricardo; GUARIENTO, Daniel Bittencourt. Inteligência artificial e responsabilidade civil dos robôs. 25 out. 2019. Disponível em: https://migalhas.uol.com.br/coluna/impressoes-digitais/313834/inteligencia-artificial-e-responsabilidade-civil-dos-robos. Acesso em: 22 jun. 2020.

hipótese, tanto aquele que dispôs de recursos para o desenvolvimento do produto, como o programador, e aquele que tratou os dados inseridos na máquina (controlador) certamente deverão ser responsáveis. Isto porque a conclusão da máquina para tomar determinada decisão causadora do dano (representando o elemento "nexo de causalidade") foi feita a partir de toda essa "cadeia de produção" (investimento, tratamento de dados e programação), ainda que a partir dos dados inseridos não houvesse direta ou expressamente a determinação de que errônea decisão assim fosse deliberada.

Além disso, é válido ressaltar que, havendo contrato de consumo entre as partes, nesse caso, tanto as figuras mencionadas (desenvolvedor e controlador) quanto o fornecedor do produto deverão responder solidariamente, independentemente de culpa, nos termos dos artigos 12 e 18, do Código de Defesa do Consumidor:

> Art. 12. O fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos.
> Art. 18. Os fornecedores de produtos de consumo duráveis ou não duráveis respondem solidariamente pelos vícios de qualidade ou quantidade que os tornem impróprios ou inadequados ao consumo a que se destinam ou lhes diminuam o valor, assim como por aqueles decorrentes da disparidade, com a indicações constantes do recipiente, da embalagem, rotulagem ou mensagem publicitária, respeitadas as variações decorrentes de sua natureza, podendo o consumidor exigir a substituição das partes viciadas.

No segundo contexto acima mencionado (mau uso do *software),* se houver relação de consumo, porém, não há óbice para isenção de responsabilidade do programador e fornecedor, nos termos do artigo 12, § 3º. O fabricante, ou o construtor, ou o produtor, ou o importador só não será responsabilizado quando provar: III - a culpa exclusiva do consumidor ou de terceiros.

Por outro lado, analisando as bases legislativas já existentes e, em especial, o Código Civil, deverá ser aplicada a responsabilidade objetiva quando a atividade desenvolvida por aquele que detém o "bolso profundo" implicar riscos a terceiros, conforme preceituado no parágrafo único do artigo 927:

> Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.

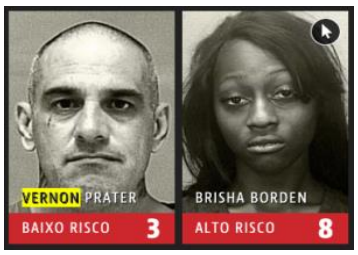
Isto porque, ao analisar os métodos de aprendizado de máquina, é justo afirmar que as atividades praticadas por máquinas inteligentes implicam riscos aos direitos de terceiros, pois

ainda não há conhecimento exato de como as decisões automatizadas são tomadas, de modo que sempre haverá incerteza sobre o resultado. Então, havendo dano, mostra-se adequada a aplicação da responsabilidade objetiva daquele que aufere lucros com a venda de produtos e/ou serviços inteligentes, que, de alguma forma, possam causar prejuízo aos usuários.

A título de exemplo, há um caso em que um algoritmo, nos Estados Unidos, classificou uma pessoa negra, como mais perigosa que uma branca, apesar dos crimes desta serem demasiadamente mais graves:

> De um lado, Vernon Prater, de 41 anos, que foi pego roubando uma loja de ferramentas, o que causou um prejuízo de U$ 86,35 à vítima. Trata-se de um meliante que já havia sido condenado por assalto à mão armada mais de uma vez, além de ostentar outras inúmeras contravenções penais na sua ficha criminal.
> De outro lado, Brisha Borden, de 18 anos, que atrasada para levar sua irmã à escola pegou uma scooter que pertencia a um menino de 6 anos. Flagrada, caiu da pequena moto e foi presa por assalto. O que eles têm em comum? Ambos foram classificados por um programa de computador que previa a probabilidade de cometerem novos crimes no futuro. Borden, que é negra, foi classificada como de alto risco e Prater, que é branco, como de baixo risco. Abaixo a imagem deles, que deixa claro que o algoritmo foi preconceituoso ao realizar a classificação[4]:[23]

FIGURA 02[24]



Para comparação, a ficha criminal de ambos:

FIGURA 03[25]

[23]MOREIRA, Manoela. *Congresso mantém veto direto a uma explicação humana na LGPD. 03 out. 2019*. Disponível em: https://noticias.cers.com.br/noticia/congresso-mantem-veto-a-direito-a-uma-explicacao-humana-na-lgpd/. Acesso em: 22 jun. 2020.
[24]MOREIRA, Manoela. *Congresso mantém veto direto a uma explicação humana na LGPD. 03 out. 2019.* Disponível em: https://noticias.cers.com.br/noticia/congresso-mantem-veto-a-direito-a-uma-explicacao-humana-na-lgpd/. Acesso em: 22 jun. 2020.
[25]MOREIRA, Manoela. *Congresso mantém veto direto a uma explicação humana na LGPD. 03 out. 2019*. Disponível em: https://noticias.cers.com.br/noticia/congresso-mantem-veto-a-direito-a-uma-explicacao-humana-na-lgpd/. Acesso em: 22 jun. 2020.

Não há justificativa plausível para a decisão tomada pelo algoritmo. Considerar que tenha sido inserido qualquer conceito discriminatório no robô não seria inteligível, até porque, se examinado à luz da legislação brasileira, poderia ser considerado crime (artigo 20, lei 7.716/89), além de se tratar de violação de princípio constitucional, qual seja: a promoção do bem a todos, independentemente de raça ou cor (artigo, 3º, IV, Constituição Federal).

Outro exemplo já muito próximo da realidade são as decisões tomadas por veículos autônomos. O dilema do trem desgovernado que tem a opção de continuar o caminho e matar cinco pessoas, ou desviar do percurso e matar apenas uma, é cada vez mais real e trará diversas repercussões no cenário jurídico.

Até mesmo no campo da medicina, os procedimentos cirúrgicos, cada dia mais automatizados, deve-se considerar que, ainda que haja menos chances de uma máquina vir a erro, quando comparado à ação humana, não significa que esse tipo de sinistro (evento futuro e incerto) não virá a acontecer, uma vez que estão em constante aprendizado, como já debatido. Enfatiza-se, ainda, que nessa área nenhum dado, ação e, consequentemente, nenhuma reação, podem ser generalizadas, justamente porque cada paciente e cada procedimento são únicos, devendo, portanto, ser tratados de forma individualizada.

As falhas, em qualquer dos exemplos acima, certamente ensejam naturalmente o entendimento do motivo pelo qual a máquina errou por parte do prejudicado, e isso não poderá ser esclarecido de forma inequívoca. Isso porque, conforme afirmam os autores Marcelo Santiago Guedes e Henrique Felix de Souza Machado:

> [...] o desempenho dessa rede não se dá a partir da programação inicial, mas das massas de dados nos quais a rede neural é treinada. Pode-se dizer, então, que o modelo de aprendizado ou de desenvolvimento não é orientado a regras de negócio ou serviços, mas aos dados.[26]

[26]GUEDES, Marcelo Santiago; MACHADO, Henrique Felix de Souza. Veículos autônomos inteligentes e a responsabilidade civil nos acidentes de trânsito no Brasil. Volume 02. Brasília. *ESMPU*, 2020. p. 48. Disponível em: http://escola.mpu.mp.br/a-escola/comunicacao/noticias/esmpu-lanca-publicacao-sobre-responsabilidade-civil-nos-acidentes-com-veiculos-autonomos/veiculos-autonomos-inteligentes.pdf. Acesso em: 07 nov. 2020.

Não é possível saber como a máquina chegou ao resultado dos casos mencionados. Daí a necessidade de revisão humana, bem como da responsabilidade objetiva, daquele que possui o "bolso profundo" e, por conseguinte, daquele que dispôs de recursos financeiros suficientes para criar e programar o algoritmo, o que já se aproxima da legislação existente.

6 PROPOSIÇÕES CONCLUSIVAS

Baseando-se nos fatos apresentados e demais discussões a respeito do tema, resta evidente a importância de haver a possibilidade de uma revisão feita por pessoa natural, ou, mesmo, regulamentar a decisão automatizada como exceção, tal como observado na GDPR, pois ainda não se sabe se uma máquina é capaz de valorar os fatos. Ou seja, é importante que se tome uma decisão que leve em consideração o ordenamento jurídico e, portanto, uma decisão legal (o que muitas já fazem, uma vez que o texto da lei é inserido no robô), mas, concomitantemente, a situação de fato, e suas respectivas individualidades.

Enquanto não existirem meios seguros que permitam o conhecimento inequívoco sobre o aprendizado de uma máquina, as revisões de decisões automatizadas deveriam ser obrigatoriamente humanas. Ressalta-se ainda a importância da redução desse tipo de decisão em procedimentos individualizados. O motivo disso se dá porque, ainda que os seres humanos sejam falhos, são também os únicos capazes de valorar uma situação, aplicando-se aquilo que se mostra razoável diante da situação fática, além de possuir a capacidade de fundamentar os motivos pelos quais a decisão foi tomada, que naturalmente será questionada pelo prejudicado. Essa ação oportuniza que esta parte venha a compreender e sopesar a situação diante da qual o responsável se encontrava. Somente dessa maneira será possível, inclusive, mensurar o valor de eventual dano moral.

Assim, considerando que o presente trabalho não busca esgotar o tema, diante de todas as teses debatidas, é possível afirmar que, enquanto o artigo 20 da Lei Geral de Proteção de Dados estiver vigente sem dispor da obrigatoriedade da revisão humana em decisões emitidas de maneira automática, a imputação da responsabilidade civil objetiva àquele que detém o *"deep-pocket"* seria ideal e sensata, com as devidas ressalvas quando se tratar de relações consumeristas, nas quais o Código de Defesa do Consumidor deve ser aplicado conjuntamente à legislação civil. Subsidiariamente, poderia o país adotar o mesmo entendimento da União Europeia (Art. 22, GDPR) em relação ao tema, isto é, autorizar as decisões automatizadas de maneira excepcional.

REFERÊNCIAS BIBLIOGRÁFICAS

BARROS, Pedro. Aprendizagem de Maquina: Supervisionada ou Não Supervisionada? **Medium**, 07 abr. 2016. Disponível em: https://medium.com/opensanca/aprendizagem-de-maquina-supervisionada-ou-n%C3%A3o-supervisionada-7d01f78cd80a. Acesso em: 19 jun. 2020.

BRASIL. **Lei 10.406 de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF: Presidência da República**.** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em 20 ago. 2021.

BRASIL. **Lei 8.078 de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República**.** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 20 jun. 2020.

BRASIL. **Lei 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados. Brasília, DF: Presidência da República**.** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 20 jun. 2020.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1998**. Brasília, DF: Presidência da República**.** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em 20 jun. 2020.

DANTAS, Aldemiro. Responsabilidade Civil para leigos (brevíssima noção). **Jus Brasil**, 2013. Disponível em: https://aldemirodantas.jusbrasil.com.br/artigos/121935826/responsabilidade-civil-para-leigos-brevissimanocao#:~:text=Como%20se%20v%C3%AA%2C%20portanto%2C%20para,ou%20imprudente%20(com%20culpa). Acesso em: 20 jun. 2020.

DATA SCIENCE ACADEMY. O Que é Aprendizagem Por Reforço? Capítulo 62**. Deep Learning Book Brasil**. Disponível em: http://deeplearningbook.com.br/o-que-e-aprendizagem-por-reforco/. Acesso em: 19 jun. 2020.

FERREIRA, Osiel. Responsabilidade civil subjetiva e responsabilidade civil objetiva**. Jus**, fev. 2018. Disponível em: https://jus.com.br/artigos/64351/responsabilidade-civil-subjetiva-e-responsabilidade-civil-objetiva#:~:text=Enquanto%20que%20na%20teoria%20subjetiva,sem%20culpa%20ou%20pela%20atividade. Acesso em: 20 de jun. 2020.

FLOR, Geovano Prudêncio. Responsabilidade Objetiva do Estado. **Jus**, nov. 2016. Disponível em: https://jus.com.br/artigos/53769/responsabilidade-objetiva-do-estado#:~:text=A%20responsabilidade%20objetiva%20%C3%A9%20aquela,buscar%20a%20exist%C3%AAncia%20da%20culpa. Acesso em: 20 jun. 2020.

FRAZÃO, Ana; MULHOLLAND, Caitilin. **Inteligência artificial e direito, ética, regulação e responsabilidade.** 2ª tiragem. São Paulo: Editora Thomson Reuters, 2019.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro:** responsabilidade civil. 14. ed. São Paulo: Saraiva Jur, 2019. Vol. 4.

GUARIENTO, Daniel Bittencourt; MARTINS, Ricardo Maffeis. Inteligência artificial e responsabilidade civil dos robôs. **Migalhas**, 25 out. 2019. Disponível em: https://migalhas.uol.com.br/coluna/impressoes-digitais/313834/inteligencia-artificial-e-responsabilidade-civil-dos-robos. Acesso em: 22 jun. 2020.

GUEDES, Marcelo Santiago; MACHADO, Henrique Felix de Souza. Veículos Autônomos Inteligentes e a Responsabilidade Civil nos Acidentes de Trânsito no Brasil**.** Volume 2. Série de pesquisas. **Esmpu**. Disponível em: http://escola.mpu.mp.br/a-escola/comunicacao/noticias/esmpu-lanca-publicacao-sobre-responsabilidade-civil-nos-acidentes-com-veiculos-autonomos/veiculos-autonomos-inteligentes.pdf.

INTELIGÊNCIA. In: **MICHAELIS, Dicionário Brasileiro da Língua Portuguesa**. São Paulo: Editora Melhoramentos, 2021. Disponível em: https://michaelis.uol.com.br/busca?r=0&f=0&t=0&palavra=intelig%C3%AAncia. Acesso em: 29 nov. 2021.

LEI GDPR EM PORTUGUÊS**. Galvão & Silva Advocacia**,19 jul. 2018. Disponível em: https://www.galvaoesilva.com/lei-gdpr-em-portugues/. Acesso em: 20 jun. 2020.

MAGRANI, Eduardo. **A Internet das Coisas.** 1ª ed. Rio de Janeiro: Editora FGV, 2018.

MAGRANI, Eduardo. Máquina que pensa. **Eduardo Magrini,** 21 mar. Disponível em: http://eduardomagrani.com/maquina-que-pensa/. Acesso em: 19 jun. 2020.

MOREIRA, Manoela**.** Congresso mantém veto a direito a uma explicação humana na LGPD. **Cers**, 03 out. 2019. Disponível em: https://noticias.cers.com.br/noticia/congresso-mantem-veto-a-direito-a-uma-explicacao-humana-na-lgpd/. Acesso em: 22 jun. 2020.

O CÉREBRO É UM MODELO ÚTIL PARA A INTELIGÊNCIA ARTIFICIAL? **Brainniac**, 14 jun. 2020. Disponível em: http://www.brainniac.ufv.br/index.php/o-cerebro-e-um-modelo-util-para-a-inteligencia-artificial/. Acesso em: 22 jun. 2020.

PARLAMENTO EUROPEU COGITA CRIAR CONTRATAÇÃO COMPULSÓRIA DE SEGURO DE RESPONSABILIDADE CIVIL PARA INTELIGÊNCIA ARTIFICIAL**. Cnseg**, 27 dez. 2017. Disponível em: https://cnseg.org.br/noticias/parlamento-europeu-cogita-criar-contratacao-compulsoria-de-seguro-de-responsabilidade-civil-para-inteligencia-artificial.html. Acesso em: 21 jun. 2020.

PERSONALIDADE JURÍDICA. **Wikipédia, a enciclopédia livre**. Disponível em: https://pt.wikipedia.org/wiki/Personalidade_jur%C3%ADdica. Acesso em: 21 jun. 2020.

SILVA, Leonardo Werner. Internet foi criada em 1969 com o nome de "Aparnet" nos EUA. **Folha de São Paulo**, 12 ago. 2001. Disponível em: https://www1.folha.uol.com.br/folha/cotidiano/ult95u34809.shtml#:~:text=A%20internet%20foi%20criada%20em,Departamento%20de%20Defesa%20norte%2Damerican. Acesso em: 18 jun. 2020.

LGPD: AGENTES DE TRATAMENTO, RESPOSÁVEL E ANPD

LGPD: TREATMENT AGENTS, RESPONSIBLE AND ANPD

ANA PAULA MELLO[1]
GIOVANNA COELHO MIRAMONTES[2]

SUMÁRIO: 1. INTRODUÇÃO. 2. O CONTROLADOR E O OPERADOR. 3. O ENCARREGADO. 4. A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. 5. A RESPONSABILIDADE E O RESSARCIMENTO. 6. PROPOSIÇÕES CONCLUSIVAS. REFERÊNCIAS BIBLIOGRÁFICAS.

RESUMO

Em função da lei geral de proteção de dados no Brasil, aprovada em agosto de 2018, o objetivo deste artigo é analisar os novos cargos profissionais e órgãos públicos que surgirão a partir do momento de sua execução. O texto procura demonstrar como a LGPD pode influenciar a vida profissional do brasileiro, criando áreas de atuação, além de explicar as funções e regulamentações acerca desses novos agentes de tratamento.

Palavras-chave: LGPD; ANPD; controlador; operador; encarregado.

ABSTRACT

Due to the general data protection law in Brazil, approved in August 2018, the purpose of this article is to analyze the new professional positions and public bodies that will arise from the moment of its execution. The text seeks to demonstrate how the LGPD can influence the professional life of Brazilians, creating areas of activity, in addition to explaining the functions and regulations regarding these new treatment agents.

Keywords: LGPD; ANPD; controller; operator; foreman.

1 INTRODUÇÃO

Desde o surgimento da internet, em 1969, muitos aspectos da vida do ser humano vêm se modificando cada vez mais. Entre eles, está a constante e crescente exposição a qual se submetem ao disporem de seus dados, seja em redes sociais, ou em simples termos de uso e

[1]Estudante do 2º ano diurno do curso de graduação em Direito na Faculdade de Direito de Sorocaba e integrante do Grupo de Pesquisa em Direito Digital do ano de 2020, da Instituição.
[2]Estudante do 3º ano noturno do curso de graduação em Direito na Faculdade de Direito de Sorocaba e integrante do Grupo de Pesquisa em Direito Digital do ano de 2020, da Instituição.

política de privacidade, o que ocasiona inúmeros benefícios e facilitadores para o dia a dia, mas também traz uma série de riscos, que se tornam cada vez mais evidentes ao decorrer da evolução da tecnologia moderna. Como resultado, o direito passou a abranger o espaço digital, visando a mitigação desses riscos com a criação de leis específicas de proteção de dados, como a General Data Protection Regulation, nos países da Europa, ou a Lei Geral de Proteção de Dados, no Brasil.

A GDPR é um conjunto normas que regulamenta a coleta e o uso de dados pessoais de indivíduos que se encontram na União Europeia, e é considerada uma evolução do diretivo 95/46 CE, de 1995, já existente na Europa, e regulamento mundialmente pioneiro em relação à proteção geral de dados. A lei estava em tramitação desde 2012, e foi aprovada em 2016 pelo Parlamento Europeu, entretanto só entrou em vigor em 25 de maio de 2018, tendo um período de dois anos entre a aprovação e a vigência, justamente para que as empresas pudessem se adequar às novas regras.

Por consequência, o Brasil e muitos outros países fora da União Europeia foram influenciados a criar legislações semelhantes, uma vez que uma das exigências da GDPR é a de que os dados só poderiam ser transferidos para outros países ou organizações internacionais se estes tivessem leis adequadas de proteção de dados. Sendo assim, o governo brasileiro sancionou, no dia 14 de agosto de 2018, a LGPD, sendo sua vigência prevista para 2022, sob motivação semelhante à da GDPR.

Certamente, a LGPD prevê diversas inovações, entre elas novos cargos profissionais, dado que obriga determinadas empresas a designar agentes de tratamento de dados, como controlador, operador e encarregado, com a função de monitorar os dados fornecidos por clientes, bem como mitigar qualquer tipo de risco existente. Dessa maneira, o presente artigo tem como objetivo esclarecer as funções e responsabilidades desses novos agentes, tal como analisar seus impactos na sociedade.

2 O CONTROLADOR E O OPERADOR

Primeiramente, é cabível ressaltar a importância dos agentes de tratamento, que são fundamentais para que haja a eficácia da LGPD, além de serem um instrumento essencial para a promoção de uma cultura de proteção de dados pessoais dentro da instituição. Ademais, esses agentes são responsáveis por propor políticas e conscientizar todos os agentes internos envolvidos com o tratamento de dados pessoais, gerenciando e fiscalizando processos que envolvem o tratamento desses dados. Não por acaso, em julho de 2019, a Federal Trade

Comission exigiu que o Facebook nomeasse tais agentes e criassem um comitê de privacidade independente de seu conselho diretor, o que representaria um importante aliado no fortalecimento da estruturação e implantação de práticas transparentes de tratamento de dados pessoais.

Assim sendo, é possível definir os agentes de tratamento que a LGPD traz, sendo eles o controlador e o operador, ambos responsáveis pelo tratamento de dados dentro das empresas e organizações, porém com funções distintas. O artigo 5º da lei fixa o controlador como uma pessoa física ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais. Já o operador também pode ser uma pessoa natural ou jurídica, de direito público ou privado, contudo sua função é realizar o tratamento de dados pessoais em nome do controlador.

Um exemplo concreto dessa situação se dá quando uma empresa de call center (operador) é contratada por um banco (controlador) para coletar dados pessoais de seus clientes. O banco irá passar à empresa a decisão a respeito de quais dados devem ser apurados (como nome, endereço, entre outros) e, em seguida, essa empresa irá operar a coleta em nome do banco. Posto isto, o controlador é o responsável por tomar as decisões relacionadas ao tratamento de dados pessoais de uma determinada entidade pública ou privada, visando a concordância com as exigências da LGPD e a mitigação dos riscos (por exemplo, o vazamento de dados, por falha de medidas de segurança).

Dessa maneira, na etapa do processo de tratamento de dados pessoais, a função do controlador será decidir quais dados a entidade irá coletar, por qual meio, qual a finalidade da coleta, quais as políticas de retenção de dados e quais os receptores desses dados, caso existam. Isto é, retomando ao exemplo do banco, será de sua responsabilidade decidir quais dados pessoais de seus clientes serão coletados, uma vez que é o controlador, assim como deverá decidir por qual meio (telefone, internet, carta), levando sempre em consideração a finalidade e o modo mais seguro de realizar a coleta.

Além disso, uma de suas responsabilidades é elaborar relatórios de impacto à proteção de dados pessoais (RIPD), que consiste em uma documentação que expõe todos os processos de tratamento de dados, com a finalidade de comprovar a eficácia do tratamento e a conformidade com a lei. Esse relatório apoia o princípio da prestação de contas e ajuda a provar que a empresa tomou as medidas técnicas e organizacionais apropriadas e necessárias. Esse documento, no entanto, não exime a responsabilidade da empresa em casos de vazamento de dados e, havendo falha na condução adequada do RIPD nos casos em que a lei

determina a sua obrigatoriedade, constituirá violação de lei, podendo resultar em multas administrativas. Para exemplificar, um controlador que não elabora adequadamente o RIPD, ao se deparar com uma situação de vazamento de dados de um determinado cliente, além de responder pelo dano causado, possivelmente responderá por uma multa administrativa, ou seja, o prejuízo será dobrado.

Similarmente, o operador é o responsável por realizar o tratamento dos dados pessoais em nome do controlador e de acordo com as decisões tomadas por este. Dessa forma, sua obrigação é seguir à risca todas as instruções concedidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria. Alguns aspectos relevantes sobre a dinâmica desses dois agentes na LGPD é que, ao contrário da GDPR, não é necessário nenhum contrato formal para estabelecer essa submissão do operador em relação ao controlador, ela é presumida. Além disso, ele responderá solidariamente com o controlador pelos danos causados quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas fornecidas.

Outra discussão a respeito se refere à possibilidade de uma pessoa ser o controlador e o operador simultaneamente, já que a lei não positiva tal situação. Entretanto, tendo como base a GDPR, que inspirou a LGPD, há um dispositivo que estabelece que não seria apropriado um sujeito ser controlador e operador ao mesmo tempo, para o mesmo conjunto de dados e para o mesmo tratamento. É certo que tais circunstâncias gerariam dificuldades na hora de definir as funções e responsabilidades administrativas de cada parte, contudo ainda não há regulamentação específica para essa conjuntura.

Em suma, a diferença essencial entre essas duas posições é o poder de decisão, posto que o controlador a tem, e o operador, não. À vista disso, o operador é considerado um subordinado do controlador, levando em conta que deve executar suas ordens, enquanto este apresenta-se no topo da cadeia de tratamento de dados.

3 O ENCARREGADO

É de suma importância examinar também a figura do encarregado pelos dados pessoais, ou também conhecido como “Data Protection Officer” (DPO). Segundo o artigo 5° da LGPD, o encarregado é uma pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Cabe ressaltar que o DPO não é considerado um agente de tratamento, mas deve atuar em conjunto com estes, efetuando um papel de intermediário.

Consequentemente, o encarregado, após nomeado pelo controlador, com sua identidade e informações divulgadas publicamente, deve exercer suas funções, definidas pelo §2° do artigo 41 da LGPD. São essas funções, portanto: aceitar reclamações e comunicações dos titulares, prestar esclarecimentos, adotar providências, receber comunicações da autoridade nacional, orientar funcionários e contratados da entidade sobre as práticas a serem tomadas em relação à proteção de dados pessoais e executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Para ilustrar, em 2018, a empresa "Marketdata", que trabalha com marketing orientado a dados, ou seja, CRM, *Business Intelligence*, *Business Analytics* e Inteligência Artificial para gerar resultados de engajamento e vendas para grandes marcas, contratou Claudinei Vieira para o cargo de DPO, que, dentro da empresa, relatou que exerce as seguintes funções: organização de dados e de inventário dos clientes, qualificação de dados sensíveis, revisão das políticas de privacidade da empresa, além de representação dessas políticas perante a autoridade nacional.

À vista de suas funções, torna-se possível traçar o perfil do encarregado, que é essencial, uma vez que as suas ações estarão diretamente relacionadas à imagem da organização. Primeiramente, é necessário certo conhecimento em determinadas funções de TI, como práticas de proteção de dados do setor, processamento de dados, entre outros. Ademais, é preciso uma especialização em leis e práticas nacionais de proteção de dados, incluindo uma compreensão profunda da GDPR – no caso do Brasil, da LGPD, fora as demais atribuições que cabe à empresa fornecer ao encarregado, como um conhecimento intenso da organização e um livre acesso à alta administração no que se referir à proteção de dados.

Por fim, é necessário frisar os tipos de empresa que devem nomear um encarregado ou DPO. No caso da LGPD, é determinado que todas as empresas e os profissionais liberais devem possuir um responsável "encarregado" ou "DPO" para garantir que o dispositivo seja seguido à risca. Contudo, o artigo 41, §3°, estipula que a ANPD pode estabelecer hipóteses de dispensa da indicação do encarregado para determinadas empresas, dependendo do tamanho da empresa ou do volume de dados processados.

4 A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

A Autoridade Nacional de Proteção de Dados é o órgão central para a interpretação e fiscalização da LGPD e de essencial fator para a eficácia da lei, podendo-se dizer que este está para o setor de proteção de dados, assim como a ANATEL está para o setor de

telecomunicações. Salienta-se que, por ser um órgão federal, sua aplicação se dá em todo o território nacional e sua criação está prevista no artigo 55-A[1] da Lei Geral de Proteção de dados: "Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República."

De acordo com o artigo 55-J da LGPD, a ANPD tem 24 competências no total, dentre elas destacam-se: zelar pela proteção dos dados pessoais, fundamentando-se na LGPD, promover o conhecimento da população acerca da proteção de dos dados pessoais e das ações de medidas preventivas de segurança, desenvolver diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, articulando estudos e considerando sempre as condutas internacionais de proteção de dados pessoais e privacidade, fiscalizar a aplicação da lei, bem como aplicar sanções nos casos de descumprimento, comunicando irregularidades às autoridades, avaliar as reclamações enviadas pelos usuários, realizar termos de compromissos com órgãos a fim de eliminar possíveis irregularidades, além de criar mecanismos para que os usuários possam registrar suas reclamações de maneira simples.

Uma peculiaridade acerca da ANPD é a de que, após dois anos, sua natureza poderá ser alterada, podendo ser uma autarquia vinculada à Presidência da República, ficando tal alteração a critério do governo, isto é, a sua natureza é transitória. Sua estrutura organizacional é composta por diversos setores da sociedade, como estabelece o artigo 55-C da LGPD, sendo constituída pelos seguintes cargos: o Conselho Diretor, considerado o órgão máximo de direção, que será representado por 5 diretores que terão mandatos variáveis, de dois a seis anos, sendo seus membros selecionados entre brasileiros com nível superior de educação, reputação ilibada e reconhecimento notável no campo de especialidade dos cargos que serão nomeados; o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, composto por 23 representantes, titulares e suplentes, de órgãos públicos e da sociedade civil, não remunerados e com o mandato de dois anos; a Corregedoria; a Ouvidoria; o órgão de assessoramento jurídico próprio e unidades administrativas necessárias à lei.

Cabe ressaltar que a primeira diretoria da ANPD foi aprovada pelo plenário do senado em outubro de 2020, sendo o diretor-presidente nomeado Waldemar Gonçalves Ortunho Junior, formado em engenharia eletrônica pelo Instituto Militar de Engenharia, pós-graduado em engenharia elétrica pela Universidade de Brasília e em pedagogia pela Universidade de Quito, o qual terá um mandato de seis anos. Além da referida indicação, outros quatro nomes foram confirmados para compor o conselho diretor da ANPD: Arthur Pereira Sabbat, formado

em comunicações, com mandato de cinco anos, a advogada Miriam Wimmer, com mandato de dois anos, a advogada Nairane Farias Rabelo Leitão, com mandato de três anos e Joacil Basilio Rael, graduado em artilharia.

5 A RESPONSABILIDADE E O RESSARCIMENTO

Já estabelecida a função do controlador e do operador, assim como sua atuação na área, é cabível analisar a sua responsabilidade no caso de descumprimento da lei. Ambos, quando derem causa a algum tipo de dano, podendo ser patrimonial, moral, individual ou coletivo, são obrigados a repará-lo. A fim de assegurar a efetiva indenização ao titular dos dados, o operador e/ou controlador podem responder solidariamente pelos danos causados. Só não haverá responsabilização por parte dos agentes de tratamento quando provarem que não foram estes responsáveis por realizar o tratamento de dados, ou mesmo que o tenham realizado sem nenhuma violação à lei. Existe, porém, a possibilidade de o dano ter sido causado pelo titular dos dados.

É importante ressaltar que o tratamento de dados será ilegal quando se deixar de observar a legislação ou quando não se oferecer o mínimo de segurança que o titular espera. As circunstâncias mais relevantes e observadas são o modo pelos quais o tratamento de dados é realizado, o resultado e os riscos que se esperam e as técnicas de tratamento de dados pessoais disponíveis conforme a época, ou seja, se a tecnologia evoluiu em um determinado tempo, a forma com a qual o tratamento de dados é realizado deve ser melhorada simultaneamente.

Consoante os artigos 42 ao 45, o legislador buscou não apenas determinar o ressarcimento de danos, mas principalmente buscou prevenir e evitar a ocorrência de tais feitos. Para que os danos sejam indenizáveis, há de ser resultante de uma violação de qualquer dispositivo da lei, não importa de qual parte, ou se for de um titular ou não. Os protagonistas da lei são os controladores e operadores, que são obrigados a reparar os danos específicos, se estes forem causados. Já a vítima não se resume somente em quem é o titular de dados, podendo então ser qualquer pessoa que sofra algum prejuízo resultante da violação da LGPD.

6 PROPOSIÇÕES CONCLUSIVAS

Dado todos os fatos, concluímos que a LGPD precisa ser colocada em vigência o mais rápido possível, pois os desvios causados com os dados pessoais são recorrentes e não há nada específico que assegure o titular, o operador e o controlador, por isso a lei é de suma

importância nesse caso. Também é importante lembrar os novos empregos que surgirão por meio da lei, como o próprio controlador, o operador, o DPO. Outrossim, aumentará a demanda da área de TI, o que seria muito importante para auxiliar no atual cenário de desemprego do Brasil. Internacionalmente, o Brasil também seria bem visto, pois foi através da EU que surgiu esta lei, e consequentemente o país receberia mais propostas que contribuiriam com a economia do país, porque mutuamente os dados estariam assegurados por lei.

Visto os impactos que a LGPD causará na sociedade ao longo dos anos, entre eles está um crescente processo de expansão e padronização econômica de consumo. Isto porque a LGPD surgiu em um cenário globalizado, em que a Europa deu a iniciativa de uma lei de proteção de dados, de modo que o Brasil se viu com a mesma necessidade; tendo isso ocorrido, poderá ocorrer o mesmo com a economia. É um lento processo de mudança e adequação, mas a economia mundial mudará conforme a LGPD e GDPR, pois através delas se dispõem mais oportunidades de comercialização entre os países, por isso acabou sendo a proteção interna que cada país tem a responsável por regular os dados para sua mercadoria.

Em suma, esse acontecimento é muito importante para haver mais proteção e fiscalização entre importações e exportações feitas em nosso país. Com a LGPD, surgem mais chances de um comércio seguro e padronizado, no sentido de que outros países terão de se submeter a mesma segurança e fiscalização.

REFERÊNCIAS BIBLIOGRÁFICAS

BORELLI, Alessandra *et al*. **LGPD Comentada**. 3. ed. São Paulo: Revista dos Tribunais, 2021.

BRASIL**.** Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. **Autoridade Nacional de Proteção de Dados**. Brasília, DF: Presidência da República, 2021.

DONDA, Daniel. **Guia Prático de Implementação da LGPD**. São Paulo: Editora Labrador, 2020.

O LIMITE DO TRATAMENTO DE DADOS SEM O CONSENTIMENTO DO TITULAR

THE LIMIT OF DATA PROCESSING WITHOUT THE OWNER'S CONSENT

SABRINA LUMI FURUCABA[1]

SUMÁRIO: 1. INTRODUÇÃO. 2. O CONSENTIMENTO. 3. A INEXIGIBILIDADE DO CONSENTIMENTO. 4. CONSENTIMENTO DE CRIANÇAS E ADOLESCENTES. 5. PESQUISA DE CAMPO. 6. O TRATAMENTO DE DADOS PELO PODER PÚBLICO. 7. RESPONSABILIDADES. 8. CONSIDERAÇÕES FINAIS. REFERÊNCIAS BIBLIOGRÁFICAS**.**

RESUMO

A Lei Geral de Proteção de Dados é a primeira Lei brasileira que dispõe acerca do tratamento de dados pessoais, tendo sua criação inspirada na GDPR, legislação de origem europeia. Um dos assuntos abordados na Lei é o Consentimento, tema central do presente artigo, que tem como definição a aprovação necessária para a realização de tratamento de dados. Para o tratamento de dados de crianças e adolescentes, existem alguns pontos a serem observados. No artigo, abordam-se também as hipóteses de inexigibilidade do consentimento do titular, em especial o tratamento de dados realizados pelo Poder Público, e por fim, acerca das responsabilidades em casos de vazamento de dados.

Palavras-chaves: LGPD; Consentimento; Tratamento de dados dessoais; Proteção de dados.

ABSTRACT

The General Personal Data Protection Law is the first Brazilian law that regulates the processing of personal data, the creation was inspired by the GDPR, legislation of European origin. One of the subjects regulated in the Law is Consent, the central theme of this article. Consent is the approval required to data processing. For the treatment of personal data from children and adolescents, there are some points to be observed. The article also addresses the hypotheses of non-enforceability of the holder's consent, in particular the processing of data executed by the Public Authority, and finally, about the responsibilities in cases of data leak.

Keywords: LGPD; Consent; Personal Data Processing; Data Protection.

[1]Estudante do 3º ano diurno do curso de graduação em Direito na Faculdade de Direito de Sorocaba e integrante do Grupo de Pesquisa em Direito Digital do ano de 2020, da Instituição.

1 INTRODUÇÃO

A Lei Geral de Proteção de Dados - LGPD (Lei nº 13.709/2018) - é a primeira legislação no Brasil que dispõe, especificamente, sobre o tratamento de dados pessoais, com o objetivo de proteger os direitos fundamentais da liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural.

O país já possui a Lei n° 12.965/2014, denominada Marco Civil da Internet - MCI, uma lei ordinária que antecedeu a LGPD, e que tem como característica ser mais ampla e geral, pois regula o uso e o acesso à internet genericamente, sem muitas especificações.

Inspirada no *General Data Protection Regulation* (GDPR), legislação criada pela União Europeia, que entrou em vigor no dia 25 de maio de 2018, a LGPD tem como objetivo proporcionar o controle dos dados pessoais e a privacidade dos usuários, concentrando a atenção na segurança dos dados armazenados. Com isso, os usuários passam a ter o poder de permitir ou não o tratamento de dados pelos controladores.

Os dados pessoais, os dados sensíveis, bem como o seu respectivo tratamento é o tema central da LGPD, e são definidos das seguintes formas: artigo 5º, inciso I da LGPD: dado pessoal: informação relacionada a pessoa natural identificada ou identificável, ou seja, é o que permite identificar uma pessoa.

Os dados pessoais sensíveis são dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, à saúde ou à vida sexual, à genética ou biométrica, quando vinculado a uma pessoa natural. Conforme afirma Bruno Bioni, o dado pessoal sensível é "uma espécie de dados pessoais que compreendem uma tipologia diferente em razão de o seu conteúdo oferecer uma especial vulnerabilidade, discriminação". O tratamento de dados consiste em toda ação realizada com os dados pessoais, que engloba desde a coleta, bem como a produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Uma das disposições que a LGPD aborda está relacionada ao consentimento, tema central deste artigo.

2 O CONSENTIMENTO

O consentimento referente ao tratamento dos dados é um assunto abordado tanto no MCI, quanto na LGPD. No entanto, houve uma mudança na adjetivação do consentimento,

pois o MCI estabeleceu que a coleta, o uso, o armazenamento e o tratamento dos dados pessoais devem ocorrer mediante o consentimento expresso do titular. Em contrapartida, a LGPD define o consentimento como manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Dessa maneira, o consentimento seria expresso se os usuários pudessem, através de um chat ou algum canal similar, por exemplo, manifestar de forma explícita a sua concordância em relação aos termos e condições de uso. Entretanto, pode-se obter também o consentimento por meio das condutas socialmente típicas, e por este fato a LGPD emprega o termo inequívoco.

MCI Nº 12.965/ 14	LGPD - Lei n°13709/18
Art. 7º, inciso IX da MCI - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;	Art. 5°, inciso XII da LGPD - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

Conforme exposto acima, na LGPD o consentimento é a permissão que o titular concede para determinada pessoa física ou jurídica, de natureza privada ou pública, para realizar o tratamento de dados pessoais, de modo que as informações obtidas devem ser utilizadas somente para finalidade específica determinada. Para se obter um consentimento válido, é necessário preencher todos os requisitos previstos na forma da lei, de forma livre, informada, inequívoca e específica, obedecendo também os requisitos previstos no Direito Civil, como o da capacidade jurídica. Sem todos estes requisitos, o consentimento não pode ser considerado válido.

Caso ocorram mudanças nos termos de uso e na política de privacidade, o agente de tratamento deve informar o titular e obter um novo consentimento. Ademais, o titular possui também o direito de revogar o consentimento a qualquer momento, mediante manifestação expressa do titular, ou seja, quando ocorrer alguma alteração e eventualmente o titular não concordar com o novo termo, ele pode revogá-lo, conforme sua vontade, sem qualquer ônus.

3 A INEXIGIBILIDADE DO CONSENTIMENTO

A LGPD traz as hipóteses que dispensam o consentimento do titular, descritas no artigo 7°:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem)
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

4 CONSENTIMENTO DE CRIANÇAS E ADOLESCENTES

Com relação aos dados de crianças e adolescentes, estes estão inseridos em uma categoria de dados especiais, uma vez que a legislação exige a aplicação de procedimentos específicos para o tratamento.

Segundo o Estatuto da Criança e do Adolescente (Lei nº 8.069/90), considera-se criança a pessoa até doze anos de idade incompletos, e adolescente aquela entre doze e dezoito anos de idade. Desse modo, observa-se que as crianças e os adolescentes são aqueles que civilmente são considerados absolutamente incapazes e relativamente incapazes respectivamente.

No caput do artigo 14 da LGPD, dispõe que o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse. Ademais, o parágrafo do mesmo artigo, estabelece que as informações sobre o tratamento de dados de crianças e adolescentes devem ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Além do princípio da finalidade e transparência, o dispositivo leva em consideração o princípio do melhor interesse, integrando o ordenamento jurídico brasileiro e buscando atender prioritariamente aos interesses e direitos dos menores. Por meio dele, pode-se observar a vulnerabilidade que cerca os menores, ressaltando-se o dever da família, da sociedade e do Estado em proteger a privacidade, que é um dos direitos das pessoas envolvidas.

No tocante ao consentimento, a LGPD no parágrafo 1º, do artigo 14, estipula que o tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. Observa-se que o artigo somente menciona as crianças, pois quanto aos adolescentes não há exigência de especificidades para obtenção do consentimento. Diante disso, verifica-se que a norma vigente determina uma proteção maior para as crianças em relação aos adolescentes, com a exigência do consentimento livre e inequívoco do responsável legal.

Ademais, o parágrafo 5º do artigo 14 dispõe o dever do controlador em realizar todos os esforços razoáveis para verificar se o consentimento foi dado pelo responsável pela criança, visto que o ambiente virtual está passível de maneiras de burlar os meios de identificação. Assim, cabe aos controladores constatar a validade e a legitimidade do consentimento. Conforme aduz o parágrafo 6º do mesmo artigo, são hipóteses de inexigibilidade do consentimento específico em casos nos quais a coleta é necessária para contatar os pais ou o responsável legal, sendo utilizada uma única vez e sem armazenamento, ou de proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento.

Outrossim, as hipóteses previstas no artigo 7º da LGPD também podem ser aplicadas para as crianças e adolescentes. Em determinadas circunstâncias, como é o caso da tutela da saúde da criança, é dispensado o consentimento específico para tratamento, se porventura o responsável legal não estiver presente. Além disso, é vedada a prática de compartilhamento indevido dos dados a terceiros sem o consentimento.

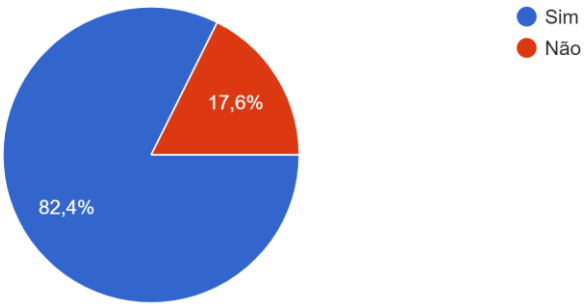
Vale ressaltar que, na era conectividade digital, as crianças, especificamente da geração Z em diante, convivem com o mundo digital desde o seu nascimento. Por causa da presença ativa no ambiente on-line sem a devida supervisão, aumentam-se os riscos de exposição. Em comparação com as gerações passadas, por exemplo, que não tinham tecnologia digital disponível, as crianças e adolescentes estão muito mais vulneráveis ao vazamento e ao uso ilegal de seus dados pessoais.

5 PESQUISA DE CAMPO

A pesquisa de campo foi realizada com 85 pessoas, por meio da plataforma Google Forms, de forma anônima, com o objetivo de verificar o conhecimento acerca da existência da LGPD.

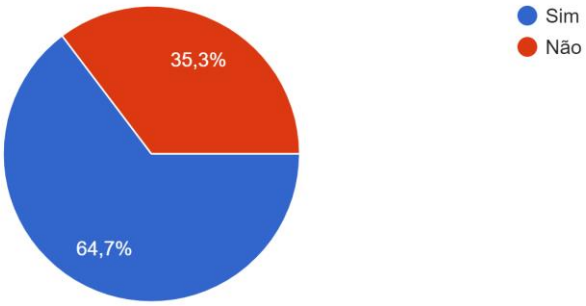
3. Aceita o termo sem ler mesmo, pois é cansativo e não entende nada.

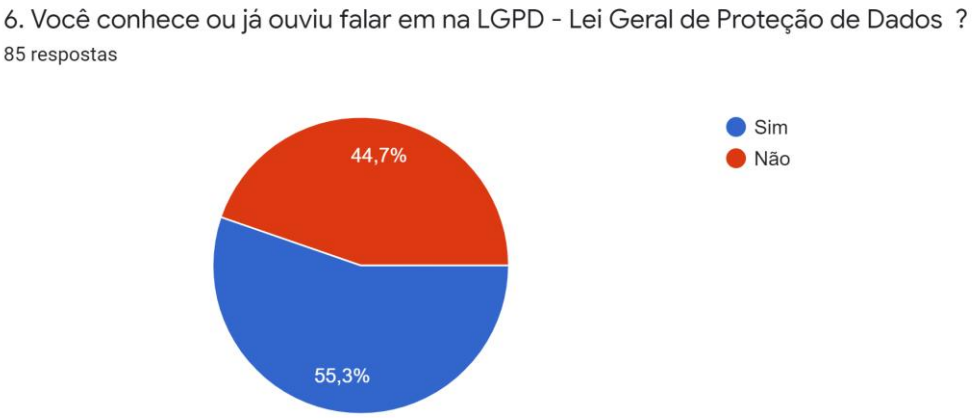
85 respostas



4. Você sabe para que esse termo serve ?

85 respostas





O resultado da pesquisa demonstrou que a maioria dos participantes da pesquisa, mesmo não sendo operadores do direito, tem conhecimento da LGPD. Além disso, uma grande parte não acredita na segurança dos sites na internet, contudo, não possui o costume de realizar a leitura completa dos termos de uso, onde se obtém o consentimento acerca do tratamento de dados pessoais.

Dessa forma, a amostragem que foi obtida na pesquisa de campo revela que o consentimento é muito frágil. As pessoas preocupam-se com a segurança de suas informações pessoais, contudo não há preocupação e cuidado suficientes para se atentarem ao conteúdo dos termos de uso. Percebe-se que o que ocorre é a falsa ideia de que nada de grave irá acontecer com as suas informações pessoais.

6 O TRATAMENTO DE DADOS PELO PODER PÚBLICO

Conforme previsto no artigo 7° da LGPD, o poder público, em algumas situações, pode tratar os dados sem o consentimento do titular. Esse tratamento de dados pessoais deve seguir as diretrizes propostas pelo artigo 23 da mesma lei, nas quais as pessoas jurídicas de direito público devem atender apenas a sua finalidade e o interesse público. Além disso, a Medida Provisória n° 954, de 2020, publicada pelo Presidente da República, é um caso que pode ser utilizado como exemplo para verificar o limite que a norma tem posto ao Poder Público.

A MP 954/2020 tratava sobre o compartilhamento de dados por empresas de telecomunicações durante a emergência de saúde pública causada pelo Covid-19. A situação de calamidade pública afetou várias esferas do Direito, incluindo o Direito Digital. Tal Medida tinha como objetivo compartilhar dados de usuários por prestadoras de serviços de telecomunicações com o Instituto Brasileiro de Geografia e Estatística (IBGE), para dar suporte à produção estatística oficial durante a pandemia do novo coronavírus.

Como previsto na Lei, o poder público poderia de forma lícita tratar os dados pessoais sem o prévio consentimento dos titulares, visto que se trata de uma questão de tutela da saúde e da vida da população, desde que fosse verificado minuciosamente o modo como esse tratamento ocorreria. O que entra no jogo neste caso é a segurança dos dados pessoais frente ao tratamento sem consentimento do titular.

A MP 954/2020 teve sua eficácia suspensa pela ministra Rosa Weber, do Supremo Tribunal Federal (STF). A relatora deferiu medidas cautelares solicitadas em cinco Ações Diretas de Inconstitucionalidade, propostas pelo Conselho Federal da Ordem dos Advogados do Brasil (ADI 6387), pelos seguintes partidos: Partido da Social Democracia Brasileira (ADI 6388), Partido Socialista Brasileiro (ADI 6389), Partido Socialismo e Liberdade (ADI 6390) e Partido Comunista do Brasil (ADI 6393).

O argumento principal de destaque utilizado pela ministra é proteção constitucional dos artigos 1°, III e 5º, X e XII, da Constituição Federal que ampara o direito à intimidade, à vida privada, à honra, à imagem das pessoas, ao sigilo de dados e à autodeterminação, afirmando a existência de vícios de inconstitucionalidade formal. Acrescenta, ainda, que a MP não tem nenhuma previsão que estabeleça exigências quanto aos procedimentos e sistemas que asseguram o sigilo, à rigidez e ao anonimato dos dados compartilhados, o que não atende a efetiva proteção de direitos fundamentais dos brasileiros, determinadas na Constituição Brasileira. Ressaltou também a inexistência do interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia. Com isso, o

deferimento da medida cautelar da ministra teve como finalidade prevenir danos irreparáveis à intimidade e ao sigilo da vida privada dos usuários dos serviços de telefonia.

Um ponto de destaque nesse caso é a questão da revogabilidade do titular, um dos direitos do titular. A MP produz efeitos jurídicos imediatos, ou seja, possui força de lei; contudo, necessita da posterior apreciação pelas Casas do Congresso Nacional (Câmara e Senado) para se converter definitivamente em lei ordinária. Sem a aprovação das Casas legislativas, ela não tem efeito. Ainda assim, é possível que a MP passe a se tornar uma lei ordinária, o que resultaria em efeitos de uma obrigação legal, de modo que o titular não poderá solicitar que os seus dados não sejam tratados, diferentemente das relações privadas, em que não existe tal imposição do Poder Público.

Outro caso concreto para exemplificação é a decisão sobre a implementação de um sistema de câmeras com reconhecimento facial pela Companhia Do Metropolitano De São Paulo - Metrô. O tema central da decisão sobre a Produção Antecipada da Prova não é o consentimento, todavia, em um dos itens, a juíza Renata Barros Souto Maior, da 1ª Vara de Fazenda Pública de São Paulo, solicita que o Metrô apresente prova documental sobre qual consentimento foi dado, pelos usuários, para uso de suas informações e sobre como o Metrô obterá o consentimento dos pais ou responsáveis legais para obtenção, armazenamento e uso de dados pessoais de crianças e adolescentes, seguindo os termos do Estatuto da Criança e do Adolescente. A abordagem da juíza, na qual afirma a que o sistema de reconhecimento facial é um potencial violador de direitos constitucionais, como direito à privacidade e à autodeterminação informativa, é interessante, visto que o sistema de reconhecimento facial é uma medida de segurança pública que visa aumentar a segurança pública, que é um direito dos cidadãos. Entretanto, a implementação deste sistema viola o direito à privacidade.

Verifica-se que ambos os casos supracitados se enquadram nos requisitos que dispensam o consentimento, mas não preenchem os requisitos em relação à segurança dos dados pessoais. Ademais, em ambos os casos os legisladores priorizam a proteção dos direitos fundamentais do cidadão, utilizando-se do argumento da inviolabilidade dos direitos individuais.

7 RESPONSABILIDADES

Um tópico relevante para o tratamento de dados é a possibilidade de vazamento de dados, pois, no atual cenário que a humanidade vive, o impacto de um vazamento de dados é

muito maior se comparado com tempos passados. Atualmente, o mundo digital proporciona que as pessoas sejam muito mais conectadas, o que facilita a disseminação das informações.

Diante da situação, a LGPD dispõe que o controlador ou o operador que, no 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. A lei estabelece também algumas sanções como advertências e multas, conforme segue o artigo 52 da lei:

> 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: (Vigência)
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III - multa diária, observado o limite total a que se refere o inciso II;
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI - eliminação dos dados pessoais a que se refere a infração;
> VII - (VETADO);
> VIII - (VETADO);
> IX - (VETADO).
> X - (VETADO) ; (Incluído pela Lei nº 13.853, de 2019)
> (Revogado)
> (Promulgação partes vetadas)
> XI - (VETADO) ; (Incluído pela Lei nº 13.853, de 2019)
> (Revogado)
> (Promulgação partes vetadas)
> XII - (VETADO) . (Incluído pela Lei nº 13.853, de 2019)
> (Revogado)
> (Promulgação partes vetadas)
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019)

8 CONSIDERAÇÕES FINAIS

Verifica-se que o consentimento é elemento de suma importância, mas que apresenta uma fragilidade, visto que é uma conduta típica consentir com os termos de uso sem ter o conhecimento do conteúdo das condições de uso. Isto é, o titular não tem efetivamente o conhecimento do que está consentido. Esse ato pode causar danos graves como o vazamento de dados, bem como o uso indevido de suas informações pessoais.

No que diz respeito ao consentimento das crianças e adolescentes, é possível observar uma maior proteção à criança, em face ao adolescente, devido à sua vulnerabilidade. No entanto, o consentimento obtido pelo responsável da criança está passivo de fraude, considerando as tecnologias disponíveis, o que pode possibilitar o uso indevido dos dados do menor.

Não existe, por ora, um limite concreto estabelecido para o uso de dados pelo poder público. Todavia, nos dois casos citados acima, ambas demonstram que uma medida de segurança ou uma situação de calamidade no sistema de saúde podem coletar e tratar dados pessoais, de forma legal, mas que, ainda assim, não devem excluir as hipóteses para proteções de direitos fundamentais da personalidade, como o direito à proteção da privacidade, da intimidade, imagem e honra. Observa-se que a proteção dos dados pessoais sensíveis é de suma importância, e que, mesmo com a existência de base legal para uso de dados pessoais sem o consentimento, a entidade do direito público deve agir no limite da finalidade estabelecida e com a devida condição de segurança.

Como visto nos termos da lei, o tratamento de dados pessoais pode ocorrer sem o consentimento do titular, contudo o ato deve acontecer em situações nas quais seja indispensável o tratamento pelo poder público. As situações de emergências, como no caso da MP 954/2020, não podem legitimar de nenhuma forma o desprezo de garantias fundamentais consagradas na Constituição.

A LGPD visa a proteção dos direitos dos titulares, os critérios mínimos para tratamentos de dados pessoais devem ser cumpridos de forma rígida. Por fim, a relatora ressaltou que não se subestima a gravidade e a urgência decorrente da atual crise sanitária, nem a necessidade de formulação de políticas públicas que demandam dados específicos para o enfrentamento do novo coronavírus. No entanto, ela avaliou que o combate à pandemia não pode legitimar os atos.

À vista disso, a ministra Rosa Weber deferiu a medida cautelar, "a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel", e determinou que o IBGE se abstenha de requerer os dados previstos na MP e, caso já tenha solicitado tais informações, que suspenda tal pedido, com imediata comunicação às operadoras de telefonia. A decisão será submetida a referendo do Plenário.

REFERÊNCIAS BIBLIOGRÁFICAS

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. rev., atual., reformul. Rio de Janeiro: Forense, 2019.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD**)**. Brasília, DF: Presidência da República**.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: abr. 2020.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República**.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: abr. 2020.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, DF: Presidência da República**.** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: nov. 2021.

BRASIL. Ministra Rosa Weber solicita informações ao IBGE e à Anatel sobre compartilhamento de dados. **Supremo Tribunal Federal**, 2020. Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=44209. (Indisponível). Acesso em: abr. 2020.

BRASIL. Ministra suspende MP que prevê compartilhamento de dados com o IBGE por empresas de telecomunicações durante pandemia. **Supremo Tribunal Federal**, 2020. Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=442090. Acesso em: abr. 2020

BUCCO, Rafael. OAB pede no STF derrubada da MP 954, que ameaça a privacidade dos usuários de telefonia**. Telesíntese,** 2020. Disponível em: https://www.telesintese.com.br/oab-pede-no-stf-derrubada-da-mp-954-que-ameaca-a-privacidade-dos-usuarios-de-telefonia/. Acesso em: abr. 2020.

CORRÊA, Adriana Espíndola. Lei de proteção de dados e a identificação nacional: há antinomias**? Consultor Jurídico**, 2019. Disponível em: https://www.conjur.com.br/2019-fev-18/direito-civil-atual-lei-protecao-dados-identificacao-nacional-antinomias. Acesso em: abr. 2020.

GARCIA, Maria Carolina B.; NUNES, Paula Freire Santos A. Tratamento de dados pessoais de crianças e adolescentes: proteção e livre desenvolvimento do menor cercados pela LGPD e responsabilidade parental**. Instituto Brasileiro de Direito da Família**. Disponível em: https://ibdfam.org.br/artigos/1673/Tratamento+de+dados+pessoais+de+crian%C3%A7as+e+adolescentes%3A+prote%C3%A7%C3%A3o+e+livre+desenvolvimento+do+menor+cercados+pela+LGPD+e+responsabilidade+parental. Acesso em: 14 nov. 2021.

GONZÁLEZ, Mariana. O que a LGPD diz sobre o consentimento do cidadão em relação a seus dados pessoais. **Guia LGPD,** 2019. Disponível em: https://guialgpd.com.br/o-que-a-lgpd-diz-sobre-o-consentimento/. Acesso em: maio 2020.

GONZÁLEZ, Mariana. LGPD Comentada. **Guia LGPD**, 2019. Disponível em: https://guialgpd.com.br/lgpd-comentada/. Acesso em: abril de 2020.

LIMA, Cíntia Rosa Pereira de. Consentimento inequívoco versus expresso: o que muda com a LGPD? **Revista do Advogado,** N° 144, P. 60-66, nov. de 2019.

MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. **Migalhas**, 2020. Disponível em: https://migalhas.uol.com.br/coluna/migalhas-de-vulnerabilidade/329261/dados-pessoais-sensiveis-e-consentimento-na-lei-geral-de-protecao-de-dados-pessoais. Acesso em: out. 2020.

PECK, Patricia. **Proteção de dados pessoais:** comentários à Lei n. 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva, 2020.

ROVER, Tadeu. Metrô de SP tem 30 dias para apresentar documentos sobre reconhecimento facial. **Consultor Jurídico**, 2020. Disponível em: https://www.conjur.com.br/2020-fev-13/metro-sp-apresentar-documentos-reconhecimento-facial. Acesso em: maio 2020.

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

ZAPPELINI, Thaís Duarte. **Guia de proteção de dados pessoais crianças e adolescentes**. 1. ed. São Paulo: FGV, 2020. Cap. 5.

REVISÃO E ATUALIZAÇÃO DE CONTRATO SOB O PRISMA DA PRIVACIDADE E PROTEÇÃO DE DADOS

REVIEW AND UPDATE OF AGREEMENT UNDER THE PRISMA DPRIVACIDADEE AND DATA PROTECTION

SAMANTA HELOISA CARNIATO[1]

SUMÁRIO: 1. INTRODUÇÃO. 2. REVISÃO E ATUALIZAÇÃO DE CONTRATO SOB O PRISMA DA PRIVACIDADE E PROTEÇÃO DE DADOS. 3. O QUE PRECISA SER INCLUÍDO NO CONTRATO? QUAIS DETALHES SOBRE O PROCESSAMENTO O CONTRATO DEVE INCLUIR?. 4. QUAIS SÃO OS TERMOS MÍNIMOS EXIGIDOS?. 4.1 Processamento apenas nas instruções documentadas do controlador. 4.2 Dever de confiança. 4.3 Medidas de segurança adequadas. 4.4 Usando sub-operadores. 4.5 Direitos dos titulares dos dados. 4.6 Auxiliar o controlador. 4.7 Disposições de fim de contrato. 4.8 Auditorias e inspeções. 5. AS CLÁUSULAS CONTRATUAIS PADRÃO (SCCS) PODEM SER USADAS?. 6. CONCLUSÕES. REFERÊNCIAS BIBLIOGRÁFICAS.

RESUMO

Em vigor desde setembro de 2020, a Lei Geral de Proteção de Dados - LGPD (Lei 13709/2021) - determina que as empresas revisem suas operações que envolvem os dados de pessoas físicas. Sendo assim, os contratos vigentes devem passar por uma revisão com a finalidade de garantiruma segurança jurídica entre as partes em relação à proteção de dados. Nesse caso, o que importa são formas de ações de tratamento de dados pessoais que o contrato cria por meio desses deveres e obrigações, sendo obrigatório que no contrato se discorra sobre os dados pessoais e sua tutela.

Palavras-chave: Contrato; Direito; Direito Digital.

ABSTRACT

In force since September 2020, the General Data Protection Law - LGPD (Law 13709/2021) determines that companies review their operations involving data from individuals. Therefore, existing contracts must undergo a review in order to ensure legal certainty between the parties in relation to data protection. In this case, what matters are forms of actions for the processing of personal data that the contract creates through these duties and obligations, then, in the contract, it is mandatory that you talk about the personal data and its protection.

Keywords: Contract; Right; Digital law.

[1]Estudante do 5º ano diurno do curso de graduação em Direito na Faculdade de Direito de Sorocaba e integrante do Grupo de Pesquisa em Direito Digital do ano de 2020, da Instituição.

1 INTRODUÇÃO

Sabe-se que o Direito sempre está em atualização. Isso se deve ao fato de que muitos acontecimentos do cotidiano acabam por exigir uma adequação jurídica. Até alguns anos não se tinha muito conhecimento em direito digital, diferentemente da Europa, que possui há muito tempo uma regulamentação para tanto: o Regulamento Geral sobre a Proteção de Dado (GDPR). No Brasil, depois de muito tempo, surgiu a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, uma legislação geral com a finalidade de proteção de dados e privacidade dos seus cidadãos. Pela referida lei, é possível trazer conceitos jurídicos novos, como "dados pessoais", "dadospessoais sensíveis", e esses dados precisam de tratamento e por isso existem procedimentos e normas para serem realizados com segurança. A partir desses conceitos e procedimentos novos, é necessário analisar o aspecto dos contratos, pois carregam os dados pessoais e dados sensíveis das pessoas, já que, em muitos casos,não especificam o que será feito com os tipos de dados referidos.

2 REVISÃO E ATUALIZAÇÃO DE CONTRATO SOB O PRISMA DA PRIVACIDADE E PROTEÇÃO DE DADOS

Um contrato é um espaço jurídico no qual o Estado se abstém de legislar, deixando que duas partes (por padrão, com exceções) legislem entre si, criando obrigações e deveres que devem respeitar os princípios Constitucionais e Civis.

Segundo a definição de Carlos Roberto Gonçalves (2012):

> "O contrato é uma espécie de negócio jurídico que depende, para a sua formação, da participação de pelo menos duas partes. É, portanto, negócio jurídico bilateral ou plurilateral. Com efeito, distinguem-se, na teoria dos negócios jurídicos, os unilaterais, que se aperfeiçoam pela manifestação de vontade de apenas uma das partes, e os bilaterais, que resultam de uma composição de interesses. Os últimos, ou seja, os negócios bilaterais, que decorrem de mútuo consenso, constituem os contratos. Contrato é, portanto, como dito, uma espécie do gênero negócio jurídico".[2]

Sob o prisma da Privacidade e Proteção de Dados, o que realmente importa para quem faz a análise do contrato são as formas de ações de tratamento de dados pessoais que o contrato cria, isto é, por meio desses deveres e obrigações é que as partes podem manifestar sua vontade correlata e concordar. Para fins de entendimento, apenas uma distinção sobre dados pessoais e dados sensíveis:

> "Dado pessoal é qualquer informação relacionada a pessoa natural identificada ou identificável. E como exemplos: dados cadastrais, data de nascimento, profissão, dados de GPS, identificadores eletrônicos, nacionalidade, gostos, interesses e hábitos

[2]GONÇALVES, Carlos Roberto. Direito civil brasileiro, v. 3: contratos e atos unilaterais. 16. ed. São Paulo: Saraiva, 2019. Livro Digital. (1 recurso online). ISBN 9788553608546. Disponível em: https://integrada.minhabiblioteca.com.br/books/9788553608546. Página 22. Acesso em: 24 ago. 2020.

de consumo, entre outros".[3]

Assim, dados pessoais são os dados que possibilitam a identificação de uma pessoa natural. Quanto aos dados sensíveis, que a Lei Geral de Proteção de Dados também dispõe, há um tratamento mais rigoroso, pois envolvem questões íntimas do indivíduo,como origem racial ou étnica, convicção religiosa, opinião política, filiação sindical ou organização de caráter religioso, político ou filosófico. Além disso, há também dados relacionados com a saúde, vida sexual, dados genéticos ou biométricos, que possibilitam queum indivíduo possa ou não vir a sofrer discriminação e, sendo assim, necessitam do tratamento de dados sensíveis.

A própria LGPD também traz as definições:

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;[4]

Além desses incisos, tem-se também a definição de titular, controlador e operador que a própria lei traz:

> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto detratamento;
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quemcompetem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza otratamento de dados pessoais em nome do controlador;[5]

Por exemplo: é como se eu contratasse você para guardar meus dados e você contrata outra pessoa para guardar os dados que passei a você. Eu sou o controladordos dados pessoais e você é a operadora dos dados pessoais e a pessoa que você contratou é a sub operadora.

Assim, de pronto, precisa-se analisar o que Lei de Proteção de Dados (LGPD)nos diz sobre essas formas de tratamento. Conforme o artigo 5º, X, da LGPD, que prevê algumas descrições e acepções, as ações de tratamento são, em sua maioria, verbos, palavras que de alguma forma realizem algum tipo de alusão a algum tipo decontato com os dados pessoais, conforme se segue:

> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento,

[3]VRA. TECNOLOGIA, MÍDIA E TELECOMUNICAÇÕES. Cartilha Lei Geral de Proteção de Dados Pessoais. 2019. Página 04 da versão digital.
[4]Art. 5 da lei 13709/18.
[5]Art. 5 da lei 13709/18.

> eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusãoou extração;[6]

Então, se algum contrato, de alguma forma, cria uma obrigação ou dever quanto aos dados pessoais que possa ser referido nesses termos, o contrato deve, necessariamente, discorrer sobre dados pessoais e sua devida tutela. *(Anexo 01 – Exemplo de Contrato)*. Logo, pode-se entender que qualquer contrato que aborde pessoasfísicas em alguma das partes já tem a necessidade de discorrer em algum momento sobre a tutela dos dados pessoais, visto que esses dados são sempre utilizados paraa identificação das partes, já no início do contrato.

Em suma, toda e qualquer obrigação do contrato deve gerar a pergunta: "Existe algum dado pessoal nessa cláusula?". Se houver, essa cláusula deve ser analisada, visando ter certeza de que os dados pessoais ali presentes são devidamentetutelados e balizados de acordo com a base legal coerente.

Devido a essas mudanças com dados pessoais e dados sensíveis, muitas empresas necessitam de uma adaptação, com a finalidade de elaborar um plano quese adeque às novas regras.

> "Dentre as mudanças, destaca-se a necessidade de que as empresas revisem e atualizem contratos e documentos jurídicos em duas esferas, ordinária e extraordinária: a primeira dividida em (i) interna, entre os próprios funcionários; e (ii) externa, perante consumidores e fornecedores; a segunda, em relação a dados fornecidos a operadoresou colhidos de terceirizadas, bem como qualquer terceiro".[7]

No Webinar que ocorreu em 30 de abril de 2020, houve uma conversa a respeito de "Contratos e Cláusulas de Privacidade e Proteção de Dados Pessoais". Durante a palestra on-line foi abordado que a Lei Geral de Proteção de Dados (LGPD) não possui uma previsão expressa de obrigação de firmar contrato. Diferentemente da GDPR, em que há regulamentação expressa da necessidade de formar relações jurídicas de tratamento pela via do contrato. A LGPD, apesar de não possuir previsão expressa, apresenta disposições que auxiliam a enxergar que há uma obrigação implícita. O palestrante Paulo Lilla, da Lefosse Advogados, fez as seguintes observações:

> "Na GDPR, os artigos 26 e 28 regulamentam expressamente a necessidade de formar relações jurídicas entre agentes de tratamento pela via do contrato".
> (...) Apesar da LGPD não trazer a obrigação expressa de contratação entre agentes de tratamento, ela traz uma série de disposições que permitem constatar que há uma obrigação implícita para que os agentes de tratamento formalizem suas relações pela via do contrato. Não só os princípios que estão no art. 6º, que adotam os

[6]Art. 5 da lei 13709/18.

[7]CASTILHO, Marcos. LGPD: a necessidade de revisão contratual pelas empresas. Disponível em: <https://www.miller.adv.br/single-post/2019/03/28/LGPD-a-necessidade-de-revis%C3%A3o- contratual-pelas-empresas>. Acesso em: 21 ago. 2020

> controles necessários para garantir segurança em torno de dados, o artigo 18, § 6º que trata do direito, quando o responsável deverá informar de maneira imediata que tenharealizado o uso de compartilhamento de dados (...). Se o titular de dados pede a eliminação de dados para um controlador e ele tem um contrato de compartilhamento de dados, tem que ter um mecanismo contratual para fazer com que os demais controladores conjuntos ou individuais também façam essa eliminação. Então só com contrato eu consigo garantir isso".[8]

Além dessa observação, também comenta a respeito do art. 46 da LGPD.

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.[9]
> "Então quer dizer como que o controlador se assegura de que o operador que ele está contratando adote essas medidas? Isso é pela via contratual também. Ele vai botar uma clausula contratual determinando requisitos mínimos de segurança que o operador tem que adotar. A mesma coisa um contrato de compartilhamento de dados".[10]

Por fim, com base na ICO (Information Commissioner's Office), há uma apresentação de diversos pontos que poderia ser incluído em um contrato, apesar deestarem em termos da GDPR. O artigo foitraduzido do inglês para o português do Brasil (PT-BR), sendo assim:

3 O QUE PRECISA SER INCLUÍDO NO CONTRATO? QUAIS DETALHES SOBRE O PROCESSAMENTO O CONTRATO DEVE INCLUIR?

O artigo 28 (3) estabelece que o contrato (ou outro ato jurídico) deve incluir osseguintes detalhes sobre o processamento:

- O objeto e a duração do processamento;
- A natureza e o propósito do processamento; o tipo de dados pessoais e as categorias do titular dos dados; e obrigações e direitos do controlador;
- O controlador, portanto, precisa ser muito claro desde o início sobre a extensão do processamento que está contratando.

4 QUAIS SÃO OS TERMOS MÍNIMOS EXIGIDOS?

O artigo 28 (3) também estabelece os seguintes termos ou cláusulasespecíficas que devem ser incluídas no contrato:

[8]LILLA, Paulo. WEBINAR. *LGPD Acadêmico*. Contratos e Cláusulas de Privacidade e Proteção de Dados Pessoais. Disponível em: https://www.youtube.com/watch?v=5XU9BQzJcLA . Acesso em: 24ago. 2020.
[9]Art. 46 da Lei 13709/18.
[10]LILLA, Paulo. WEBINAR. *LGPD Acadêmico*. Contratos e Cláusulas de Privacidade e Proteção de Dados Pessoais. Disponível em: https://www.youtube.com/watch?v=5XU9BQzJcLA. Acesso em: 24 ago. 2020.

- Processamento apenas nas instruções documentadas do controlador.
- Dever de confiança.
- Medidas de segurança apropriadas.
- Usando operadores.
- Direitos dos titulares dos dados.
- Ajudando o controlador.
- Disposições de fim de contrato.
- Auditorias e inspeções.

Estes são os requisitos mínimos, mas o controlador e o operador podem concordar em complementá-los comseus próprios termos. Cada um desses termos é explorado mais adiante.

4.1 Processamento apenas nas instruções documentadas do controlador

Nos termos do Artigo 28 (3) (a), o contrato deve dizer que o operador só podeprocessar dados pessoais de acordo com as instruções documentadas do responsável pelo tratamento (incluindo ao fazer uma transferência internacional de dados pessoais), a menos que seja exigido de outra forma pela União Europeia ou por um membro Lei estadual.

O contrato pode incluir dados sobre as instruções especificadas no artigo 28 (3), ou essas instruções podem ser fornecidas separadamente. Uma instrução pode ser documentada usando qualquer forma escrita, incluindo e-mail. A instrução deve ser passível de ser salva, para que haja um registro da instrução. Esse termo de contrato deve deixar claro que é o controlador, e não o operador, que tem o controle geral do que acontece com os dados pessoais.

Se um operador agir fora das instruções do controlador de tal forma que decida a finalidade e os meios de processamento, incluindo o cumprimento de uma obrigação legal, será considerado um controlador em relação a esse processamento e terá a mesma responsabilidade como controlador.

4.2 Dever de confiança

Nos termos do artigo 28.(3) (b), o contrato deve indicar que o operador deve obter um compromisso de confidencialidade por parte de qualquer pessoa a quem autorize o tratamento

dos dados pessoais, a menos que essa pessoa já esteja sujeitaa tal obrigação por lei.

Esse termo do contrato deve abranger os funcionários do subcontratante, bem como quaisquer trabalhadores temporários e trabalhadores temporários que tenham acesso aos dados pessoais.

4.3 Medidas de segurança adequadas

Nos termos do artigo 28 (3) (c), o contrato deve obrigar o operador a tomar todas as medidas de segurança necessárias para cumprir os requisitos do artigo 32 relativos à segurança do tratamento.

Tanto os controladores quanto os operadores são obrigados, de acordo com o Artigo 32, a adotar medidas técnicas e organizacionais adequadas para garantir a segurança de quaisquer dados pessoais que processem, que podem incluir, conformeapropriado:criptografia e pseudonimização:

- a capacidade de garantir a confidencialidade, integridade, disponibilidade e resiliência contínuas dos sistemas e serviços de processamento;
- a capacidade de restaurar o acesso aos dados pessoais em caso de incidente;
- e processos para testar e avaliar regularmente a eficácia das medidas.

A adesão a um código de conduta ou esquema de certificação aprovado podeser usada como forma de demonstrar o cumprimento das obrigações de segurança. Códigos de conduta e certificação também podem ajudar os operadores a demonstrargarantias suficientes de que seu processamento estará em conformidade com o GDPR.

4.4 Usando sub-operadores

Nos termos do artigo 28 (3) (d), o contrato deve indicar que:

- o operador não deve envolver outro operador (ou sub operador) sem a autorização prévia por escrito específica ou geral do controlador;
- se um operador for empregado sob a autorização geral por escrito do controlador, o operador deve informar o controlador de quaisquer alterações pretendidas e dar ao controlador a chance de contestá-las;
- se o operador empregar um sub operador, deverá celebrar um contrato que

imponha as mesmas obrigações de proteção de dados do artigo 28 (3) a esse sub operador. Isso deve incluir que o sub operador fornecerá garantias suficientes para implementar medidas técnicas e organizacionais adequadas de tal forma que o processamento atenda aos requisitos do GDPR. A redação dessas obrigações não precisa refletir exatamente as estabelecidas no contrato entre o responsável pelo tratamento e o operador, mas deve oferecer um nível equivalentede proteção para os dados pessoais;

- o operador é responsável perante o controlador pela conformidade de um suboperador com suas obrigações de proteção de dados.

4.5 Direitos dos titulares dos dados

Nos termos do artigo 28 (3) (f), o contrato deve prever que o operador adote "medidas técnicas e organizacionais adequadas" para ajudar o responsável pelo tratamento a responder aos pedidos de indivíduos no sentido de exercer os seus direitos.

Essa disposição decorre do Capítulo III do GDPR, que descreve como o responsável pelo tratamento deve permitir que os titulares dos dados exerçam váriosdireitos e respondam a solicitações para fazê-lo, como solicitações de acesso do sujeito, solicitações de retificação ou apagamento de dados pessoais e objeções a emprocessamento.

4.6 Auxiliar o controlador

Nos termos do artigo 28 (3) (f), o contrato deve indicar que, tendo em conta anatureza do tratamento e as informações disponíveis, o transformador deve ajudar o responsável pelo tratamento a cumprir as suas obrigações de:

- manter os dados pessoais seguros;
- notificar violações de dados pessoais à autoridade supervisora;
- notificar violações de dados pessoais aos titulares dos dados;
- realizar avaliações de impacto da proteção de dados (DPIAs) quando necessário;
- consultar a autoridade supervisora quando um DPIA indicar que háum alto risco que não pode ser mitigado.

Recomendamos que o contrato seja o mais claro possível sobre como ooperador ajudará o controlador a cumprir suas obrigações.

4.7 Disposições de fim de contrato

Nos termos do artigo 28 (3) (g), o contrato deve indicar que, no final do contrato, o operador deve:

- à escolha do controlador, excluir ou devolver ao controlador todos os dados pessoais que tenha processado para ele;
- e deletar as cópias existentes dos dados pessoais, a menos que a legislação da União Europeia ou dos Estados-Membros exija o seu armazenamento.

Deve-se observar que a exclusão de dados pessoais deve ser feita de maneirasegura, de acordo com os requisitos de segurança do artigo 32.

O contrato deve incluir esses termos para garantir a proteção contínua dos dados pessoais após o término do contrato. Isso reflete o fato de que, em última instância, cabe ao controlador decidir o que deve acontecer com os dados pessoais que estão sendo processados, uma vez que o processamento esteja concluído.

Apreciamos a realidade prática de que pode não ser possível que os dados em backups ou arquivos sejam excluídos imediatamente na rescisão de um contrato. Desde que as proteções adequadas estejam em vigor, como os dados sendo colocados imediatamente após o uso, pode ser aceitável que os dados não sejam excluídos imediatamente se o período de retenção for apropriado e os dados sejam subsequentemente excluídos o mais rápido possível, por exemplo, no próximo ciclo de exclusão / destruição.

4.8 Auditorias e inspeções

Nos termos do Artigo 28 (3) (h), o contrato deve exigir:

- o operador deve fornecer ao controlador todas as informações necessárias para demonstrar que as obrigações previstas no artigo 28foram cumpridas;
- o operador deve permitir e contribuir para as auditorias e inspeções realizadas pelo controlador, ou por um auditor nomeado pelo controlador.

Tal disposição obriga o operador a demonstrar ao responsável pelo tratamento o cumprimento da totalidade do artigo 28. Por exemplo, o operador pode fazer isso fornecendo ao controlador as informações necessárias ou submetendo-o auma auditoria ou inspeção.

O GDPR não exige que o contrato inclua uma cláusula exigindo que o operador mantenha registros do processamento que realiza para o controlador, embora tais registros sejam úteis para o operador demonstrar conformidade com o Artigo 28. Entretanto, requisitos para os operadores manterem os registos das suas atividades de processamento são definidos no artigo 30 (2).

5 AS CLÁUSULAS CONTRATUAIS PADRÃO (SCCS) PODEM SER USADAS?

O GDPR permite que a Comissão da União Europeia e as autoridades de supervisão (como a ICO) emitam cláusulas padrão a serem incluídas em contratos entre controladores e operadores. Essas cláusulas podem fornecer uma maneira simples de garantir que os contratos entre controladores e operadores estejam em conformidade com o GDPR. Eles também podem fazer parte de um esquema de certificação para demonstrar o processamento em conformidade, quando os esquemas forem aprovados.

> A Agência Dinamarquesa de Proteção de Dados adotou SCCs que foram aprovados pela EDPB. Se você usar essas SCCs em um contrato com um operador (sem emenda), o contrato deve estar em conformidade com os requisitos do Artigo 28".[11]

6 CONSIDERAÇÕES FINAIS

Como já mencionado, a LGPD não tem expressamente uma obrigação de firmar contratos. No entanto, não se pode negar que as relações contratuais sempre vão existir juntamente com a LGDP a qual deverá ser usada justamente por causa dos tipos de dados e o tratamento que tais dados receberão. Por isso, as novas relações contratuais, ou até para revisar, devem se adequar à nova lei a fim de que haja uma maior transparência e segurança jurídica para as pessoas envolvidas na relação contratual.

ANEXO 01 – Exemplo de Contrato

- **Privacidade e Proteção de Dados**

1. A CONTRATADA se obriga a observar e seguir as normas gerais e setoriais aplicáveis ao objeto do contrato, assim como as melhores práticas de proteção dedados pessoais sempre que houver o tratamento de dados pessoais do CONTRATANTE.

2. O tratamento de dados pessoais realizado pela CONTRATADA terá como fundamentos (i)

[11]ICO - Information Commissioner's Office**.** What needs to be included in the contract?. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/contracts-and-liabilities-between-controllers-and-processors-multi/what-needs-to-be-included-in-the-contract/. Acesso em: 24 ago. 2020.

o respeito à privacidade; (ii) a autodeterminação informativa; (iii) aliberdade de expressão, de informação, de comunicação e de opinião; (iv) a inviolabilidade da intimidade, honra e da imagem; (v) o desenvolvimento econômico e tecnológico e a inovação; (vi) a livre iniciativa, a livre concorrência e a defesa do consumidor; e (vii) os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

3. A CONTRATADA realizará as atividades de tratamento de dados pessoais, nos limites contratualmente estabelecidos, que respeitem o princípio da boa-fé e os demais elencados na Lei Geral de Proteção de Dados:

i. Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular.

ii. Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

iii. Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades.

iv. Livre acesso: Permitir que os titulares de dados pessoais possam ter acesso facilitado e gratuito sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

v. Qualidade dos dados: repassar informações corretas e verdadeiras à CONTRATADA, de modo a que possa garantir, aos titulares, que seus dados estejam exatos, claros, relevantes e atualizados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

vi. Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento;

vii. Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

viii. Não discriminação: impossibilidade de realização do tratamento para fins

discriminatórios ilícitos ou abusivos;

ix. Responsabilização e prestação de contas: demonstração, quando requisitado pelo CONTRATANTE, de medidas práticas aplicadas no tratamento de dados pessoal.

4. Nenhum dado pessoal será tratado para finalidade diversa da estabelecida nomomento da coleta.

5. A CONTRATADA garante, naquilo que couber, os direitos dos titulares dos dados pessoais por elas tratados.

6. Todos os dados, informações, documentos, inclusive acadêmicos, avaliações estudantis, técnicos, jurídicos, planilhas, estudos, enfim, quaisquer documentos em geral referentes ao presente Contrato, o desenvolvimento do objeto contratual e/ou às Partes, emanados deste contrato verbalmente ou por escrito, em suporte físico ou eletrônico, serão caracterizados como Informações Confidenciais, obrigando-se a CONTRATADA a não divulgá-las, copiá-las, transmiti-las, cedê-las, vendê-las, torná-las acessíveis ou delas dispor a terceiros não envolvidos na prestação dos Serviços.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. **Cartilha Lei Geral de Proteção de Dados Pessoais**. Brasília, DF: Presidência da República, 2019.

CASTILHO, Marcos. LGPD: a necessidade de revisão contratual pelas empresas. **Miller**, 2021. Disponível em: https://www.miller.adv.br/single- post/2019/03/28/LGPD-a-necessidade-de-revis%C3%A3o-contratual-pelas- empresas. Acesso em: 21 ago. 2020.

GONÇALVES, Carlos Roberto. **Direito civil brasileiro:** contratos e atos unilaterais. 16. ed. São Paulo: Saraiva, 2019. v. 3. Livro Digital. ISBN 9788553608546. Disponível em: https://integrada.minhabiblioteca.com.br/books/9788553608546. Acesso em: 24 ago. 2020.

LILLA, Paulo (LGPD Acadêmico). Contratos e Cláusulas dePrivacidade e Proteção de Dados Pessoais. **Webinar**, 2021. Disponível em: https://www.youtube.com/watch?v=5XU9BQzJcLA. Acesso em: 24 ago. 2020.

WHAT NEEDS TO BE INCLUDED IN THE CONTRACT? **ICO - Information Commissioner's Office.** Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/contracts-and- liabilities-between-controllers-and-processors-multi/what-needs-to-be-included-in-the-contract/. Acesso em: 26 ago. 2020.

PROTEÇÃO AOS DADOS DO USUÁRIO DE SERVIÇOS DIGITAIS PELA LGPD E AS CLÁUSULAS ABUSIVAS NA POLÍTICA DE PRIVACIDADE

PROTECTION OF DIGITAL SERVICE USER DATA BY LGPD AND ABUSIVE CLAUSES IN PRIVACY POLICY

MARTA PRADO DE ALBUQUERQUE SEBASTIÃO[1]

SUMÁRIO: 1. INTRODUÇÃO. 2. PROTEÇÃO AOS DADOS PESSOAIS PELA LGPD. 3. USO DE DADOS DO USUÁRIO DE SERVIÇOS DIGITAIS POR EMPRESAS. 4. O QUE É POLÍTICA DE PRIVACIDADE. 5. CLÁUSULAS ABUSIVAS SOBRE O USO DE DADOS PESSOAIS DO USUÁRIO DE SERVIÇOS DIGITAIS NA POLÍTICA DE PRIVACIDADE. 6 PROPOSIÇÕES CONCLUSIVAS. REFERÊNCIAS BIBLIOGRÁFICAS

RESUMO

Versa o presente Artigo Científico sobre o uso da Política de Privacidade, com alusão às cláusulas abusivas em virtude da proteção ao usuário digital pela Lei 13.709/2018 (Lei Geral de Proteção de Dados ou LGPD). Traz ainda a problematização: a LGPD é o suficiente para proteger o usuário de serviços digitais de uma Política de Privacidade, com cláusulas que podem ser consideradas abusivas? Ademais, considera a hipótese do impacto da disponibilização dos dados pessoais dos usuários. O objetivo é explicar o porquê e como o Direito protege o usuário de serviços digitais das cláusulas abusivas na Política de Privacidade; especificamente demonstra ainda um panorama atual, expondo o conceito de Política de Privacidade. No desenvolvimento, é pretendida a abordagem sobre o uso prático e eficiente da LGPD, e sobre a adaptação da Política de Privacidade a esta. O método utilizado é o hipotético-dedutivo e baseia-se na pesquisa documental e bibliográfica, palestras renomadas e canais de mídia de profissionais diversos. A pesquisa conclui com uma abordagem do momento de transição, focando principalmente na Política de Privacidade e em cláusulas, que podem ser consideradas abusivas.

Palavras-chave: Direito digital; LGPD; Política de privacidade; Direito dos contratos; Cláusulas abusivas.

ABSTRACT

[1]Advogada, Encarregada de Dados, Analista de *Compliance*, Bacharel em Direito pela Faculdade de Direito de Sorocaba (FADI). Pós-graduanda em Direito Digital e *Compliance* pela Faculdade IBMEC São Paulo.

This scientific article is about the use of Privacy Policies, alluding to the abusive clauses due to the protection of digital users by Law 13.709/2018 (General Law of Data Protection or LGPD). It also brings the problematization: is the LGPD enough to protect the user of digital services from a Privacy Policy with clauses that can be considered abusive? Moreover, it considers the hypothesis of the impact of the availability of users' personal data. The goal is to explain why and how the Law protects the user of digital services from abusive clauses in the Privacy Policy; specifically, it also demonstrates a current overview, exposing the concept of Privacy Policy. In the development it is intended to approach the practical and efficient use of the LGPD and the adaptation of the Privacy Policy to it. The method used is hypothetical-deductive and is based on documentary and bibliographical research, renowned lectures, and media channels of various professionals. The research concludes with an approach to the transition moment, focusing mainly on the Privacy Policy and on clauses, which may be considered abusive.
Keywords: Digital Law; LGPD; Privacy Policy; Contracts Law; Unfair terms.

1 INTRODUÇÃO

Será abordada a utilização da Política de Privacidade, com alusão à possibilidade desse documento conter cláusulas abusivas, diante da Lei 13.709/2018 (Lei Geral de Proteção de Dados/LGPD), em específico irá expor o problema gerado pelo tratamento abusivo dos dados pessoais, que pode ocorrer logo no início da relação entre fornecedor e usuário, e até mesmo de forma pouco perceptível. Ainda, irá explorar a possibilidade desse problema ser prevenido com a ajuda do usuário.

Responderá à pergunta: a LGPD é suficiente para proteger o usuário de serviços digitais de uma Política de Privacidade, que represente uma forma de abuso no tratamento dos seus dados pessoais?

Trará reflexões a partir de questões como: o que é abarcado pela LGPD? O Direito poderá proteger o usuário dos serviços digitais? Por que os dados pessoais são atraentes para uma empresa? O que é Política de Privacidade? O que são cláusulas abusivas? A LGPD terá eficácia social?

Terá o objetivo geral de demonstrar e incentivar a reflexão, inicialmente, sobre a mudança trazida pela LGPD, e logo após, com exemplos de abusos constantes na Política de Privacidade e relacionados aos dados pessoais, pretende-se gerar reflexão sobre o uso prático e eficiente da Lei.

Especificamente o Artigo contextualizará e apresentará conceitos presentes na LGPD, logo após, irá abranger o tratamento dos dados do usuário de ferramentas e serviços digitais por empresas. Também, trará as definições de Política de Privacidade, focando principalmente na problemática das cláusulas abusivas, e explicará como as cláusulas da Política de Privacidade, que versam sobre o tratamento dos dados podem ser abusivas, com relação ao disposto na LGPD.

O estudo a ser exposto neste artigo utilizará como base o método hipotético-dedutivo, também utilizará pesquisas documentais e bibliográficas, artigos, pesquisas, palestras renomadas e canais de mídia sobre o tema abordado.

Por fim, concluirá com um panorama do desafio criado aos fornecedores de serviços digitais e da oportunidade aos usuários de mudança cultural, além da possibilidade de resultar em uma maior consciência sobre o poder e a abrangência de seus dados pessoais e direitos, expondo, ainda, a relação do desafio com a Política de Privacidade, em especial, sobre a utilização dos dados pessoais do usuário de serviços digitais.

2 PROTEÇÃO AOS DADOS PESSOAIS PELA LGPD

O contexto da criação da Lei Geral de Proteção de Dados (LGPD), advindo da adaptação do Direito ao momento social, refletiu diretamente na relação entre o usuário, o prestador de serviços digitais e o Poder Público, em específico, na Política de Privacidade.

Para ilustrar a iminência da necessidade social de regulamentação com relação ao tema, é possível citar acontecimentos que afetaram os usuários das plataformas digitais de todo mundo, seja como "vazamentos" ou mesmo como uso excessivo de informações pessoais do usuário, como: por meio do *Facebook*, sendo o caso mais famoso que envolveu a empresa *Cambridge Analytica* (desde 2014), *Target* e a adolescente grávida (2012), exposição de dados pela *Playstation Network* (2011), exposição das contas de usuários do Banco Inter (2018).

Deve-se ressaltar, então, que algumas empresas estão mais atentas à proteção de dados, por exemplo, aquelas que seguem a ISO 27001, que é uma norma internacional publicada pela *International Standardization Organization* (ISO) e descreve como gerenciar a segurança da informação em uma organização, e que tem como foco a proteção da confidencialidade, integridade e disponibilidade da informação de uma organização. Desta forma, já existe na empresa uma forma introduzida de prevenção de danos e tratamento delicado dos dados pessoais.

Observa-se a Política de Privacidade, que muitas vezes sequer exige uma expressão de concordância clara, bastando instalar um aplicativo ou entrar em um site, por exemplo, é afetada de imediato pela aplicação da nova Lei, em virtude da mudança na forma que deverão se relacionar, os usuários de serviços digitais, fornecedores, aqueles que retém dados pessoais dos usuários, e o Poder Público, como um "fiscal atuante". Sendo que os princípios norteadores dessa relação, além da boa fé, são também a base para a proteção dos dados dos usuários, sendo os princípios dispostos no art. 6° da LGPD.

Também é de suma importância que os envolvidos em uma relação de tratamento de dados, para a eficácia social da LGPD, saibam os direitos do titular dos dados pessoais, como obter do controlador, quando requisitado pelo titular, e em relação aos dados pessoais do titular: confirmação da existência de tratamento, acesso aos dados, correção de dados incompletos, inexatos ou desatualizados, anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD, 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, eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD, informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados, informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa, revogação do consentimento, nos termos do § 5º do art. 8º da LGPD (BRASIL, 2018, Art. 18º, incisos I a IX). Além de saber quais são as obrigações do controlador, como obter o consentimento livre, informado, inequívoco (plena consciência), eficiente, acessível e atrelado à finalidade.

Ainda, a eficácia social da LGPD, que seria a consciência, utilização e respeito às normas abrangidas por ela, tem como um dos pontos principais a adoção cultural da antecipação de problemas relacionados à proteção de dados pessoais, visto que o contexto inicial da elaboração da Lei foi a crescente disponibilização e utilização dos dados pessoais, e a consequente necessidade de regulamentar o tratamento desses dados. Contudo, a efetividade da norma dependerá de mudanças culturais, em ações costumeiras, por exemplo, a atenção ao que está escrito e é aceito em documentos digitais como a Política de Privacidade.

Em um contexto prático, a demonstração dos possíveis interesses de empresas nos dados pessoais traz também a reflexão sobre quais situações podem ser controladas com base na proteção dos dados pessoais, a qual por sua vez também envolve o equilíbrio dos interesses

entre o titular e o fornecedor de serviços. Ademais, ao observar a importância do assunto proteção de dados, percebe-se que os dados pessoais não só interferem nas relações comerciais como fazem parte delas, observação essa que será abordada a seguir.

3 USO DE DADOS DO USUÁRIO DE SERVIÇOS DIGITAIS POR EMPRESAS

Dentre as questões recorrentes sobre o tema do presente artigo está o fato que muitos usuários de serviços digitais não têm sequer dimensão do poder e do valor comercial dos dados que disponibilizam.

Os dados coletados são fontes de informação que, depois de tratados, podem ser usados para diversos ganhos, como por exemplo, o de saber exatamente o que um usuário procura e o quanto ele anseia por determinado serviço, objeto ou experiência. O tratamento dos dados pode ou não ser contra a lei, já que depende da destinação do dado tratado, do contexto e, principalmente, do consentimento do usuário (quando couber).

E, por ser passível de atingir diversos objetivos com o tratamento desses dados, o usuário deve ser informado de maneira clara e objetiva sobre a dimensão e o uso do dado coletado, para que não seja violado algum ou alguns dos seus direitos.

A comercialização dos dados movimenta a economia pelos benefícios, por exemplo, de auxiliar na criação de produtos mais próximos dos anseios dos usuários, porém, por mais benéfica que seja a aproximação, ela tem seus malefícios, como consequências sociais de isolamento do usuário em suas próprias preferências e ainda a possibilidade de enveredar por um caminho obscuro, de violação dos direitos, na qual o tratamento é realizado fora do propósito aceito pelo aderente do produto ou serviço.

Um exemplo mais atual e específico do poder da informação é a existência, anos atrás, de um site chamado “Tudo Sobre Todos”, que demonstra a possibilidade de se obter e comercializar dados pessoais em massa, com acesso fácil e rápido às informações, com o uso de diversas ferramentas tecnológicas e da internet, o que aumenta também a procura e o uso dos benefícios do acesso à informação, e reflete-se na importância social do tema de proteção aos dados pessoais.

Já em relação ao valor da informação, é possível observar o alto valor ou alto potencial de troca no mercado da informação, pois sendo vendida ou trocada, os interessados não precisariam utilizar mecanismos mais trabalhosos como a invasão.

Pelo exposto, o usuário, por não ser informado com clareza de como seus dados estão sendo tratados e como poderão vir a ser, ele poderá ser surpreendido com serviços que não queria ou não estava de acordo, e até mesmo por falhas na segurança, das quais não será/foi informado que poderia haver.

Ainda sobre como proceder à exposição dos seus dados pessoais, em um cenário problemático, o usuário pode ter sua vida comprometida, com um tratamento inadequado de seus dados pessoais, principalmente os dados pessoais sensíveis, atingindo, por exemplo, sua imagem, moral ou dignidade. Portanto, os dados pessoais podem ser a causa de um dano inesperado para quem os disponibiliza, sendo sua utilização uma atividade que admite riscos quando realizada por empresas.

Sobre a captação e a mercantilização de informações dos usuários, sabe-se que ela pode ir além, podendo ser usada e aplicada em programação neurolinguística e outros métodos de manipulação para atingir determinado público, um exemplo são as *Fake News*.

Atualmente, há uma forma das empresas tratarem os dados, minimizando os mencionados riscos, utilizando-se da anonimização dos dados pessoais, mas para isso também deve ser informado o tipo de tratamento que haverá e quem será o responsável por esse procedimento. Isso é importante, por exemplo, para impedir fraudes, e é necessário também mencionar que nem todo dado pode ser anonimizado, já que há técnicas adequadas para diferentes tipos de dado.

Assim, pela importância do tema para a economia, é necessária a ação do Poder Público para proteger os membros das relações e para regular as interações que envolvem dados pessoais, seja por meio da LGPD, pelo Código de Defesa do Consumidor (CDC), pelo Código Civil (CC) ou pela CRFB/88.

Porém, há de ser complementado o conhecimento sobre a forma de agir das empresas, por exemplo, analisando um documento eletrônico que deve ser apresentado logo no início da relação entre usuário e fornecedor de serviços digitais, a Política de Privacidade. Logo, apresentam-se as questões: o que ela é? Como ela se relaciona como a LGPD?

A seguir, conceitua-se Política de Privacidade que induz à reflexão sobre documentos digitais e como deverão abordar o assunto para se adequar à nova Lei.

4 O QUE É POLÍTICA DE PRIVACIDADE

A Política de Privacidade é necessária a todas as empresas que coletam informações pessoais. Ela informa quais os dados serão coletados e como, após a autorização do aderente ao

serviço proposto, serão utilizados e tratados pelo controlador e pelo operador (agentes no tratamento de dados, segundo a LGPD), ou se e como serão cedidos a terceiros.

A Política de Privacidade também disporá sobre o armazenamento das informações, ressaltando que os dados não são apenas os inseridos pelo usuário, mas também aqueles captados por ferramentas, como *cookies* (arquivos de Internet, criados por sites visitados e salvos no navegador utilizado, sendo essas informações usadas para identificar o visitante em páginas que possuem relação com os *cookies*), o que também deve ser informado quando utilizados.

O foco da Política de Privacidade é a proteção ao empreendimento digital e ao cliente, com vista também na prevenção de lides, como dito, e ao marketing empresarial, pelo aumento do grau de confiabilidade do fornecedor de serviços, sendo ainda esses documentos eletrônicos dotados de particularidades, como: assinatura eletrônica, informação de proteção das transações que podem ser feitas por *blockchain* (técnica de segurança digital, com base em conjuntos de informações, dissipadas pelo mundo, sobre transações), informação também sobre tratamento dos dados pessoais, criptografia ou processo de anonimização.

Observa-se que o Marco Civil da Internet (Lei n.º 12.965/2014) impactou diretamente no conteúdo da Política de Privacidade e demais documentos eletrônicos. Um exemplo é o disposto no Capítulo II, Art. 7°, sobre direitos e garantias assegurados aos usuários da internet.

Ademais, a partir da vigência da LGPD, a forma e o peso de importância da Política de Privacidade aumentará ainda mais, pois esse é o documento digital que deixa clara a intenção de proteger os dados pessoais da pessoa natural.

Dessa forma, há de se considerar também que recai sobre a Política de Privacidade os ditames do Código de Defesa do Consumidor, reafirmada a proteção pela LGPD, como um de seus fundamentos, por tamanha importância como disposto no art. 2º da LGPD.

Porém, em virtude da atual cultura brasileira, não é comum que os direitos e deveres em uma relação contratual sejam questionados já no momento do consentimento, e um dos motivos é a falta de uma leitura atenta antes de expressar concordância, o que poderá ter sua importância percebida somente quando houver divergência futura na relação entre as partes, por isso ressalta-se que uma das funções do contrato é prevenir abusos e refletir sobre o comprometimento das partes.

Esse tipo de situação ocorre com a Política de Privacidade, um documento digital pouco lido pelos usuários antes do aceite, e algumas vezes que sequer é apresentado antes do início do

tratamento dos dados pessoais, como por exemplo, ao se entrar em um site ou instalar um aplicativo, que mantém um link de acesso para a Política de Privacidade, mas não colhe o consentimento do usuário. Somente pelo acesso ao site, a coleta de dados pessoais já pode ter iniciado, por meio da coleta dos *cookies* do usuário, por exemplo.

Já com a LGPD, a disposição sobre o consentimento do aderente aos documentos digitais, como a Política de Privacidade, é primordial (quando couber, pois há situações onde o consentimento é mitigado, por exemplo, na situação mencionada no art. 7º, V, da LGPD), e será demonstrado pelo aceite, que deverá ser obtido pelo controlador, antes do tratamento dos dados, por demonstração do titular da manifestação livre, informada, inequívoca (plena consciência), eficiente, acessível e atrelada à finalidade. Ainda, o consentimento será específico quando envolver dados pessoais de crianças e adolescentes; e o titular deverá ser informado sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa e revogação do consentimento, nos termos do § 5º do art. 8º da LGPD.

Em síntese, o disposto sobre a LGPD, que gerou uma nova movimentação do Direito e da possibilidade de sua aplicação em conjunto com outras leis, foi apresentado na perspectiva sobre os possíveis interesses das empresas nos dados pessoais e neste capítulo explicado o conceito e a aplicação do documento digital Política de Privacidade; em seguida serão apresentadas informações sobre cláusulas abusivas relacionadas à proteção de dados, na Política de Privacidade.

5 CLÁUSULAS ABUSIVAS SOBRE O USO DE DADOS PESSOAIS DO USUÁRIO DE SERVIÇOS DIGITAIS NA POLÍTICA DE PRIVACIDADE

Em suma, a Política de Privacidade pode conter cláusulas que não estão conforme o ordenamento jurídico preceitua e que podem ser chamadas de cláusulas abusivas, e que de modo geral são definidas pela violação de direitos ou excessiva desvantagem entre as partes, sendo formulada com base na desigualdade do ganho com a relação.

A cláusula também pode ser abusiva por ser elaborada com o fim de se aproveitar da boa-fé do usuário e, no caso dos contratos de adesão, do anseio, da necessidade ou mesmo da falta de instrução e informação clara ao usuário pelo fornecedor, caso em que se torna mais "vantajoso" em primeiro momento aderir ao serviço, e por muitas vezes aceitar um documento eletrônico com excesso de termos técnicos, que cede acesso ilimitado aos dados pessoais, sem respeito aos seus direitos.

A fim de equilibrar também a relação entre fornecedor e usuário em um contrato de adesão, o Código Civil, no art. 423, dispõe que "quando houver no contrato de adesão cláusulas ambíguas ou contraditórias, dever-se-á adotar a interpretação mais favorável ao aderente".

Além disso, os usuários de serviços digitais, na hipótese de terem seus direitos violados, poderão com a LGPD contar com mais amparo, além do já existente pelas normas dispostas no Código de Defesa do Consumidor, Código Civil e Marco Civil da Internet, com base nos artigos de lei apresentados nesse artigo científico, por exemplo.

Ainda, como adendo, pode-se constatar que em atos cotidianos, como oferecer o CPF ao comprar um remédio em uma farmácia em uma espécie de "contrato oral", assim como a versão digital da situação, mais especificamente relacionada ao tema, um site de *e-commerce*, pode conter um cadastro mais explícito, onde serão fornecidos dados pessoais e ficará a pessoa sujeita às cláusulas abusivas e ao aceite sem informação alguma, sendo comum existir ainda a pressão para participar de algum "programa de benefícios exclusivos".

Uma das mudanças trazidas pela LGPD é a necessidade de mais precisão em cláusulas que antes abrangiam os dados pessoais de forma ampla, e precisarão informar claramente a extensão da finalidade e o modo do uso dos dados àquele que adere às condições do serviço a ser prestado. Outra consequência é o tratamento dos dados de natureza individual, sendo previsto o acesso aos dados "guardados" pelo fornecedor do serviço.

Ainda, com relação aos dados pessoais do usuário, a empresa que realizar o tratamento de dados e tiver estabelecimento no Brasil, oferecer serviços ao brasileiro como mercado consumidor ou coletar dados pessoais localizados no país, deverá respeitar o disposto na LGPD. Portanto, cláusulas que não estiverem de acordo serão consideradas abusivas.

Assim, como o exemplo atual de mudanças trazidas pela LGPD, é possível citar a Política de Privacidade do *Google*, que permite uma melhor análise (do site) pelo usuário e ainda fornece a possibilidade de *link* direto do usuário com as opções de fornecimento de dados, permitindo também que ocorram simples modificações sobre quais dados serão cedidos à empresa.

Também, é possível citar como exemplo atual de maior preocupação com cláusulas abusivas na Política de Privacidade diversos relatos sobre o aplicativo *FaceApp* e *TikTok*, que segundo notícias utilizaram os dados pessoais dos usuários para serviços além da finalidade do aplicativo em si, de forma livre e irrevogável.

Ademais, em relação ao *FaceApp,* após diversas reclamações pelos usuários, ocorreram recentes mudanças em sua Política de Privacidade, que agora dizem não coletar os álbuns de fotos e dispõem sobre a utilização das fotos somente para prover funcionalidade de edição de retratos do aplicativo, além da preocupação, por exemplo, em se adaptar à diretriz do GDPR.

Ao mesmo tempo, há tendência de criação de uma lei internacional com relação à proteção de dados, pela já observada aproximação ou inspiração das leis relacionadas aos dados pessoais, refletindo leis de um país em outro, em consequência da forte conexão entre diferentes povos, por conta da intensa comunicação pela internet.

Por fim, as cláusulas abusivas podem acarretar punições que não afetam somente a remuneração da empresa, que será fiscalizada pela Autoridade Nacional de Proteção de Dados (ANPD) e podem ter como punição 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, na importância máxima de R$ 50.000.000,00 (cinquenta milhões de reais) por infração (art. 52, II, da LGPD). Há também a possibilidade de suspensão e proibição total ou parcial do exercício de atividades relacionadas ao tratamento de dados (art. 52, X, XI e XII, da LGPD). Ressalta-se também que tal valor será adequado ao porte da empresa, pois a finalidade da norma é proteger os dados pessoais de forma consciente, mantendo, quando possível, os aspectos econômicos em equilíbrio, e respeitada a função social das empresas.

Também é importante mencionar que, a fim de prevenir incidentes contra a lei, as empresas podem incluir em seus trabalhos práticas, além das relacionadas, a já mencionada ISO 27001. Nesse sentido, as práticas de *compliance,* que de forma sucinta incluem tomar decisões em conformidade com a lei, observam as regras incumbidas e prezam por transparência nas relações, com o fim de preservar princípios éticos, ajudarão na inclusão eficiente, por exemplo, dos princípios como os dispostos no art. 6°, da LGPD (BRASIL, 2018, Art. 6º, incisos I a X), mencionados no início deste artigo, nos atos da empresa.

Observa-se também que no art. 52, § 1º, da LGPD, é prevista a consideração das ações preventivas, no procedimento administrativo que antecede as sanções, e também por esse motivo são interessantes para adoção em empresas, além de que incidentes relacionados à falta de proteção aos dados pessoais não abalam empresas somente pelos aspectos financeiros envolvidos, mas principalmente comprometem a sua confiança e reputação diante dos seus clientes/usuários.

6 PROPOSIÇÕES CONCLUSIVAS

Foi possível observar que, no ato inicial da relação entre fornecedor e usuário, com relação à proteção dos dados, a Política de Privacidade também sofreu e sofrerá importantes alterações, que começam logo no momento da elaboração do documento digital pelo fornecedor, que deverá estar mais atento às cláusulas e suas consequências.

Ademais, o fornecedor de serviços digitais deverá estar mais consciente dos direitos e deveres envolvidos por seus atos, tanto no ato de elaboração da Política de privacidade, como na relação futura com o usuário, que deverá ser mantida com mais transparência e de forma clara, além de cumprir o dever de se atentar as consequências e riscos de sua ação ao envolver dados pessoais dos usuários.

Também é importante ressaltar que a consciência dos usuários dos serviços digitais tem se mostrado frágil, e a LGPD traz uma resposta aos problemas relacionados à falta de proteção dos dados dos brasileiros, como uma forma de adequação das leis à realidade social atual. No entanto, a existência de cláusulas abusivas na Política de Privacidade somente poderão ser combatidas a partir da eficiente fiscalização do Poder Público, principalmente, pela difusão e pelo incentivo à população para conhecer e apropriar-se dos seus direitos e deveres. Assim, a mudança ocorrerá pela compreensão do momento presente, dos riscos e dos benefícios do uso de serviços digitais.

O presente artigo foi feito com a pretensão de incentivar a reflexão sobre novas políticas públicas e leis, como a LGPD, que acabam evidenciando a necessidade da conexão e do incentivo à consciência do tema em questão, dos usuários, fornecedores e autores da Política de Privacidade de serviços digitais, do momento que está sendo vivido, e como o Poder Público pode ser uma ferramenta de regulação útil para todos. Destarte, a demanda sobre a modificação da forma de interação entre indivíduos e a crescente exposição de seus dados pessoais, manifestando concordância e comprometendo-se (muitas vezes pela falta de informação, esta que, de fato, deveria ser disponibilizada) com uma Política de Privacidade que infringe seus direitos, como pelo desafio gerado na tentativa de equilíbrio entre os interesses dos fornecedores e dos usuários de serviços digitais, com relação ao tratamento dos dados pessoais do usuário.

Por fim, como conclusão, há oportunidade de mudança cultural e uso do Direito como forma de prevenção, seguidos por maior segurança e informação nas relações, que levam à consciência, elemento essencial para fornecedores e usuários de serviços digitais, seja para a elaboração/imposição de uma Política de Privacidade ou mesmo para aceitá-la, como um ato

inicial do tratamento dos dados pessoais a ser amparado pelo Estado à serviço e pelo anseio da sociedade.

REFERÊNCIAS BIBLIOGRÁFICAS

ALVES, Paulo. Facebook e Cambridge Analytica: sete fatos que você precisa saber**.** **Techtudo**, 24 mar. 2018, atualizado há 2 anos. Disponível em: https://www.techtudo.com.br/noticias/2018/03/facebook-e-cambridge-analytica-sete-fatos-que-voce-precisa-saber.ghtml. Acesso em: 15 jun. 2020.

BITTAR, Carlos Alberto. Os contratos de adesão e o sancionamento de cláusulas abusivas. **Biblioteca do Senado Federal**, 1990. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/175768/000449500.pdf?sequence=1&isAllowed=y. Acesso em: 2 jan. 2020.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990.** Brasília, DF: Presidência da República. Dispõe sobre a proteção do consumidor e dá outras providências, 11 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 10 ago. 2020.

BRASIL**. Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Diário Oficial da União: seção 1, Brasília, DF, ano 139, n. 8, p. 1-74, 11 jan. 2002. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm. Acesso em: 3 ago. 2020

BRASIL. **Lei nº 12.965, de 12 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 3 ago. 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 3 ago. 2020.

POLÍTICA DE PRIVACIDADE. **FaceApp**, vigente desde dez 2019, última atualização 4 jun. 2020. Disponível em: https://www.faceapp.com/privacy-pt.html. Acesso em: 2 ago. 2020.

FRAGOSO, Renan Schlichting. Cláusulas Abusivas Nos Contratos de Adesão. **Âmbito Jurídico**, 2 dez. 2019. Disponível em: https://ambitojuridico.com.br/cadernos/direito-do-consumidor/clausulas-abusivas-nos-contratos-de-adesao/. Acesso em: 3 ago. 2020.

LEAL, Rhand. O que é a ISO 27001? **27001 Academy**, 2020 Disponível em: https://advisera.com/27001academy/pt-br/o-que-e-a-iso-27001/. Acesso em: 15 jun. 2020.

O USUÁRIO DAS REDES SOCIAIS É CONSIDERADO CONSUMIDOR? **Blog Consuma seus direitos**, 26 fev. 2017. Disponível em: http://consumaseusdireitos.com.br/usuario-redes-sociais-considerado-consumidor/. Acesso em: 18 dez. 2019.

PORTO JÚNIOR, Odélio. Anonimização e pseudonimização**:** conceitos e diferenças na LGPD. **Baptista Luz Espaço Startup**, 29 maio 2019. Disponível em: https://baptistaluz.com.br/espacostartup/anonimizacao-e-pseudonimizacao-conceitos-e-diferencas-na-lgpd/. Acesso em: 1 ago. 2020.

POLÍTICA DE PRIVACIDADE. **TikTok**, última atualização jul. 2020. Disponível em: https://www.tiktok.com/legal/privacy-policy?lang=pt_BR. Acesso em: 2 ago. 2020.

POLÍTICA DE PRIVACIDADE E TERMOS DE USO: O QUE É E COMO FAZER. **Escola do Marketing Digital**, 9 de ago. 2017. Disponível em: https://blog.escoladomarketingdigital.com.br/politica-de-privacidade-e-termos-de-uso-o-que-e-e-como-fazer/. Acesso em: 18 dez. 2019.

PROTEÇÃO DE DADOS: RELEMBRE SEIS CASOS DE VAZAMENTOS. **ConectaJá**, 27 jan. 2020. Disponível em: https://conectaja.proteste.org.br/casos-de-vazamentos-de-dados/. Acesso em: 15 jun. 2020.

REIS, Priscila. Política de Privacidade e Termos de Uso após Marco Civil da Internet. **Reis Magalhães e Pereira Advogados**, 17 mar. 2016. Disponível em: http://www.rmpadvogados.com.br/politica-de-privacidade-e-termos-de-uso-apos-marco-civil-da-internet/. Acesso em: 1 ago. 2020.

SAIBA O QUE ACONTECE SE SUA EMPRESA DESCUMPRIR A LGPD. **Stefanini Group**, 8 mar. 2019. Disponível em: https://stefanini.com/pt-br/trends/artigos/saiba-o-que-acontece-se-sua-empresa-descumprir-a-lgpd. Acesso em: 15 jun. 2020.

SANTANA, Daniel Mendes Santana. Os contratos de adesão e as cláusulas abusivas. **IDEC**, 12 jul. 2012. Disponível em: https://idec.org.br/em-acao/artigo/os-contratos-de-adeso-e-as-clausulas-abusivas. Acesso em: 2 jan. 2020.

SEU CONSENTIMENTO É LEI! **Serpro**, 2020. Disponível em: https://www.serpro.gov.br/lgpd/cidadao/seu-consentimento-e-lei. Acesso em: 15 jun. 2020.

SOUZA, Ramon de. FaceApp ressurge com termos de uso atualizados: veja se é seguro usar o app. **The Hack**, 3 jun. 2020. Disponível em: https://thehack.com.br/faceapp-ressurge-com-termos-de-uso-atualizados-veja-se-e-seguro-usar-o-app/. Acesso em: 1 ago. 2020.

SOUZA, Renato. Dados pessoais de brasileiros são negociados livremente na internet. **Correio Braziliense**, 16 jul. 2018. Disponível em: https://www.correiobraziliense.com.br/app/noticia/brasil/2018/07/16/interna-brasil,695136/dados-pessoais-de-milhares-de-brasileiros-sao-negociados-na-internet.shtml. Acesso em: 24 maio 2020.

TERRACO ECONÔMICO. Big Data: Como a Target descobriu uma gravidez antes da família? **O Guia financeiro**, 2019. Disponível em: https://blog.guide.com.br/textos/big-data-como-a-target-descobriu-uma-gravidez-antes-da-propria-familia/. Acesso em: 15 jun. 2020.

TERMOS DE SERVIÇO. **TikTok**, última atualização jul. 2020.Disponível em: https://www.tiktok.com/legal/terms-of-use?lang=pt_BR. Acesso em: 2 ago. 2020.

PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA

SECURITY INCIDENT RESPONSE PLAN

JULIANA TORRES FERRAZ[1]

SUMÁRIO: 1. INTRODUÇÃO. 2. IMPACTOS GERAIS DO VAZAMENTO DE DADOS. 3. PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA. 4. SANÇÕES AO CONTROLADOR. 5. BREVE COMPARATIVO À LEGISLAÇÃO E JURISPRUDÊNCIA EUROPEIA. 6. PROPOSIÇÕES CONCLUSIVAS. REFERÊNCIAS BIBLIOGRÁFICAS.

RESUMO

O presente artigo tem por objetivo discorrer sobre a importância de uma reação rápida e efetiva na hipótese de um incidente de segurança, bem como explicitar a forma de elaboração de um plano de resposta. A problemática enfrentada pela pesquisa é fornecer elementos concretos para implementação das exigências da Lei Geral de Proteção de Dados (LGPD), haja vista que a jurisprudência brasileira ainda não se encontra consolidada. Assim, realiza-se um estudo breve de comparação com a jurisprudência e legislação europeias, especificamente, quanto à General Data Protection Regulation (GDPR). O artigo conclui que é essencial a implementação pelo controlador de dados de um plano de respostas eficaz, a fim de que o impacto das sanções previstas na LGPD seja minimizado. A pesquisa foi realizada pela técnica de pesquisa documental e bibliográfica.

Palavras-chave: Direito digital; Incidentes de segurança; Plano de resposta; Sanções; LGPD e GDPR;

ABSTRACT

This article aims to discuss the importance of a quick and effective reaction in the event of a security incident, as well as to explain how to prepare a response plan. The problem faced by the research is to provide concrete elements for implementing the requirements of the General Law of Data Protection (LGPD), given that Brazilian case law is not yet consolidated. Thus, a brief study of comparison with European jurisprudence and legislation is conducted, specifically with regard to the General Data Protection Regulation (GDPR). We conclude that it is essential that the data controller implement an effective response plan, so that the impact

[1]Estudante do 4º ano diurno do curso de graduação em Direito na Faculdade de Direito de Sorocaba.

of the sanctions provided for in the LGPD is minimized. The research was conducted by the technique of documentary and bibliographic research.
Keywords: Digital law; Security incidents; Response plan; Sanctions; LGPD and GDPR;

1 INTRODUÇÃO

Neste trabalho serão estudados alguns regulamentos da Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, que regula as atividades de tratamento de dados pessoais. Pretende-se abordar, especificamente, sobre a necessidade da elaboração de um plano de respostas a incidentes de segurança, a fim de preservar os dados do titular, em conjunto com uma análise dos meios necessários para minimizar o impacto das sanções.

Entretanto, percebe-se que a LGPD não define o que são incidentes de segurança, mas exemplifica as possíveis situações que se encaixam como incidentes, ou seja, aquelas capazes de afetar a tríade de segurança de informação, composta pela confidencialidade, integridade e disponibilidade de dados, conforme art. 46 da LGPD. É imprescindível que, para ser considerado um incidente de segurança, haja a ocorrência de diversos eventos de segurança de informação, capazes de comprometer as operações de negócios e ameaçar a segurança de informação, verificados em um curto espaço de tempo, de mesma origem, em uma tentativa de acesso por força bruta.

O tema torna-se mais presente no século XXI, visto que, frequentemente, é possível observar casos de perda ou roubo de dispositivos físicos, perda ou roubo de documentos com dados pessoais, acesso não autorizado de dados, divulgação inadvertida ou realização de golpes para utilização de dados. A presente situação é decorrente da revolução tecnológica, iniciada entre o final dos anos 1950 e dos anos 1970, com a expansão do uso de computadores digitais. Todavia, a regulação dessas medidas permanecia ainda muito precária, contando atualmente com as primeiras bases de um efetivo controle seguro de dados por meio da LGPD. É perceptível que os controladores de dados ainda não dispõem de um conhecimento vasto sobre o tema, haja vista que a jurisprudência ainda não se encontra estabelecida.

Sendo assim, pretende-se conduzir uma análise da forma mais adequada para implementação de um controle prévio e posterior de vazamento de dados, pela elaboração de um plano de respostas, a fim de diminuir os impactos das sanções aplicadas pela LGPD, por meio de uma breve comparação com a legislação e jurisprudências europeias.

2 IMPACTOS GERAIS DO VAZAMENTO DE DADOS

O impacto do vazamento de dados afeta pessoas físicas e jurídicas, com danos morais e materiais. Para os agentes de tratamento, os riscos são inúmeros, como perda do controle dos dados, desvalorização no mercado de ações, danos reputacionais e, consequentemente, sua difícil recuperação. Além disso, haverá aplicação de sanções e a necessidade de notificação de órgãos reguladores e de entidades. Quanto aos titulares, verificar-se-ão danos psicológicos, financeiros, emocionais, somados de discriminação, extorsão, fraudes e até mesmo roubo de identidade. Em suma, os riscos podem ser divididos em três grupos, quais sejam: riscos jurídicos, reputacionais e operacionais.

Na gama de riscos jurídicos, provavelmente se verificará uma multiplicação de ações, promovidas pelos titulares de dados expostos, assim como investigações e sanções por parte das autoridades responsáveis, tal como a Secretaria Nacional do Consumidor (Senacon) e o Ministério Público, bem como constantes ações coletivas e a ocorrência de violação a cláusulas contratuais. No que se refere aos riscos reputacionais, percebe-se que os procedimentos das empresas passarão a ser questionados. Ainda, na ocorrência de um incidente, é muito provável que ocorra a exposição desta nos meios de comunicação. Além disso, quanto aos prejuízos operacionais, a consequente perda de ativos e as perdas operacionais.

O tema tem grande relevância entre as instituições financeiras, fato este potencializado com a recente criação dos bancos digitais. Sabe-se que o Banco Inter, em 2018, sofreu um relevante incidente de segurança, capaz de vazar dados de diversos clientes. Diante desse episódio, o Banco Inter alegou pela inexistência de ataque hacker, justificando que o vazamento teria ocorrido por meio de pessoa autorizada internamente. Ocorre que nenhuma justificativa foi capaz de controlar as consequências do vazamento de dados de milhares de clientes, em que se forneceu acesso a informações pessoais, senhas, cópias de cheques, imagens de contratos, chaves de segurança, entre outros. Em suma, percebeu-se que o Banco Inter não protegeu adequadamente os dados pessoais dos clientes e daqueles que mantiverem transações bancárias.

A situação motivou a Comissão de Valores Mobiliários (CVM) a entrar com um processo contra o Banco Inter. Além disso, o Ministério Público do Distrito Federal ajuizou uma ação civil pública por danos morais, com amparo no artigo 14, parágrafo 1º, do CDC, no qual prevê a responsabilidade do fornecedor de serviços, independentemente da existência de culpa. Lembre-se, ademais, que o Código de Defesa do Consumidor é aplicável às instituições financeiras, conforme definido pela Súmula 297 do STJ, e que as instituições financeiras

respondem, objetivamente, pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros, no âmbito de operações bancárias, de acordo com o disposto na Súmula 479 do STJ.

Outrossim, a Comissão de Proteção dos Dados Pessoais do Ministério Público do Distrito Federal e Territórios ajuizou uma ação civil pública por danos morais coletivos contra o Banco Inter S/A, requisitando a condenação no pagamento de 10 milhões de indenização, visto que a ré não tomou os cuidados necessários de segurança de dados pessoais de milhares de indivíduos, clientes e não clientes. Na ocasião, sabe-se que o Banco não avisou às autoridades acerca do acontecimento, ao falhar contra um dos pressupostos básicos de um plano de resposta aos incidentes de segurança, os quais serão analisados de forma mais detalhada adiante.

3 PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA

A atuação preventiva contribui para a diminuição da ocorrência de incidentes, que, por consequência, minimiza o impacto dos prejuízos ao responsável. A LGPD, na seção de "Boas Práticas e de Governança", descreve uma série de providências a serem tomadas para situações concretas. Nesse sentido, aqueles que se atrasarem nessas adequações estarão em dissonância com a GDPR Europeia (General Data Protection Regulation) e a própria LGPD.

Essas medidas se demonstram ainda mais essenciais no momento da aplicação das sanções, visto que a existência de prevenção se torna um diferencial para o abrandamento das penalidades. Nas condenações por danos morais, por exemplo, o que se demonstra é que quando a organização não fez nada para impedir o dano, o arbitramento é definido em valores altíssimos se comparados aos que a organização agiu para impedi-los, ou quando o titular foi informado e se buscou identificar e responsabilizar o responsável. Assim sendo, é importante verificar um recente julgado do Tribunal de Justiça do Estado de São Paulo, em que houve majoração dos danos morais, devido à grave violação à intimidade e à privacidade:

> APELAÇÃO – AÇÃO CONDENATÓRIA – PRESTAÇÃO DE SERVIÇOS EDUCACIONAIS – VAZAMENTO DE DADOS PESSOAIS POR PREPOSTO – CELULAR DA AUTORA PASSADO A UM TERCEIRO – RECEBIMENTO DE MENSAGENS DE ASSÉDIO SEXUAL – RECURSO DE AMBAS AS PARTES – LEGITIMIDADE PASSIVA DA RÉ – RESPONSABILIDADE PELOS DANOS DECORRENTES DA VIOLAÇÃO AO TRATAMENTO DE DADOS PESSOAIS – LEI GERAL DE PROTEÇÃO DE DADOS **– DANOS MORAIS EVIDENTES – MAJORAÇÃO – GRAVE VIOLAÇÃO À INTIMIDADE E À PRIVACIDADE** 1 – A empresa controladora de dados pessoais é figura legítima para figurar no polo passivo de demanda que objetive a indenização pelo vazamento de dados da autora orquestrados por preposto da ré, que repassou o celular da autora para um colega

> para fins de assédio sexual (LGPD, art. 42). 2 – A ré, ao dar causa ao vazamento de dados, responde pelos danos morais sofridos (LGPD, art. 5º, VI e 42, caput). 3 – É cabível a indenização por danos morais, considerando a violação grave ao direito à intimidade e à privacidade causado pela quebra do dever de proteção de dados pessoais, o que propiciou assédio sexual agressivo. 4 – **Indenização majorada, pois a gravidade da situação, a séria negligência da empresa, a postura recalcitrante em reconhecer o erro, e a incipiente jurisprudência estadual autorizam resposta mais enérgica.** Valor de dez mil reais que se mostra mais condizente com o cenário narrado. RECURSO DA RÉ NÃO PROVIDO. RECURSO DA AUTORA PROVIDO. (TJSP; Apelação Cível 1006311-89.2020.8.26.0001; Relator (a): Maria Lúcia Pizzotti; Órgão Julgador: 30ª Câmara de Direito Privado; Foro Regional I - Santana - 8ª Vara Cível; Data do Julgamento: 01/09/2021; Data de Registro: 01/09/2021) "grifo nosso".[2]

Nesse viés, percebe-se que é imprescindível a criação e aplicação de um plano de resposta aos incidentes, que, em síntese, divide-se em três etapas: preparação, resposta e avaliação.

A *preparação* é uma etapa prévia de medidas anteriores a um possível incidente, em que ocorre a confecção de um documento com todos os procedimentos a serem adotados, incluindo as devidas atribuições aos agentes no processo de resposta. Nessa fase, torna-se fundamental a criação de um *"war room",* ou seja, um comitê de gestão de crise, responsável por tomar as medidas necessárias nas primeiras horas de um incidente, composto por perfis de diversas áreas, como compliance, jurídico, recursos humanos, negócios, além de representantes de tecnologia e segurança de informação.

Entende-se que os membros desse comitê serão estabelecidos por uma questão de estruturação interna, mas recomenda-se que, ao menos, estejam presentes o encarregado ou o DPO (*Data Protection Officer)*[3] e os demais agentes das áreas de controle. Eventualmente, poderá ser preciso contar com profissionais externos, especializados, que devem ser antevistos, deixando-os de *standy by* para atuarem imediatamente quando ocorrer um episódio.

Veja-se que o papel do *Data Protection Officer (DPO)* é essencial, aquele que é encarregado de cuidar das questões referentes à proteção dos dados da organização e seus clientes, o qual deve supervisionar o responsável pelo tratamento, a fim de que cumpra as obrigações estabelecidas em lei. Nos termos do art. 5º, inciso VIII, da LGPD é o: "encarregado: pessoa indicada pelo controlador e operador para atuar como canal de

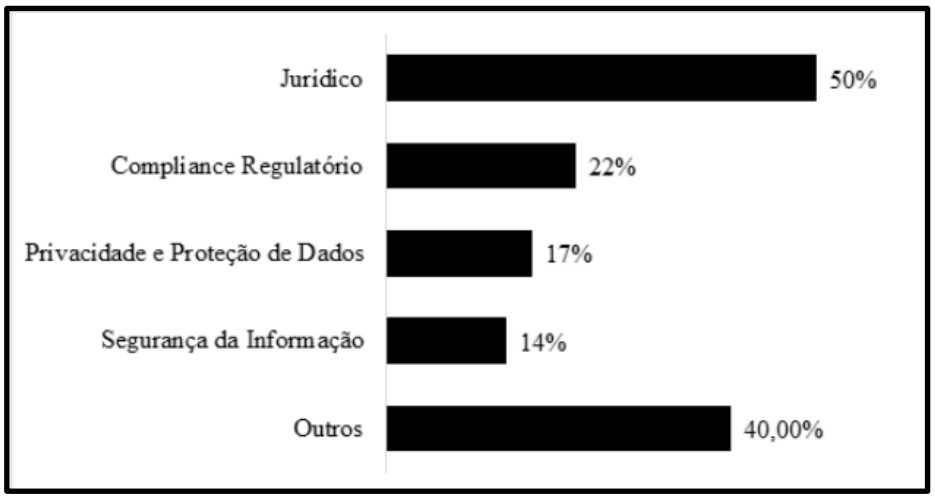
[2]BRASIL. TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO. Apelação Cível 1006311-89.2020. 8.26.0001. Relatora Maria Lúcia Pizzotti. 30ª Câmara de Direito Privado. Foro Regional I - Santana, 8ª Vara Cível. 01/09/2021. Disponível em: https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=14982708&cdForo=0. Acesso em 24 nov. 2021.

[3]Oficial de Proteção de Dados.

comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)". Aliás, é imprescindível considerar que o ponto de referência sempre será o DPO, de modo que este deve estar atento às atuações do controlador de dados ou da organização.

Dessa maneira, torna-se necessário apontar o resultado da pesquisa publicada pela *International Association of Privacy Professionals*[4] (IAPP), da divisão de funções de privacidade nas organizações, em que se percebe um comitê com alta força jurídica (50%):

Figura 1[5]



Ainda nessa etapa de preparação, treinamentos devem ser realizados, por meio dos quais são simulados incidentes de segurança, a fim de pôr os procedimentos à prova. Deverá haver um mapeamento e a manutenção dos registros das operações de tratamento de dados pessoais, identificando-se, assim, o volume e a criticidade dos dados tratados, permitindo uma organização mais eficiente e também verificando os riscos jurídicos, em uma etapa chamada de "registro das operações".

Posteriormente, deverá ser instaurada a etapa de *resposta*, ou seja, o acionamento do plano firmado em um caso concreto de incidente de segurança. Para tanto, sugere-se a elaboração de um *checklist* de ações imediatas e de esquemas, para facilitar a ação e não ocorrerem descuidos. De modo imediato, assim que um incidente de segurança for detectado,

[4]Traduzido para Associação Internacional de Profissionais de Privacidade.
[5]BLUM, Opice. E-book: Melhores práticas de Governança e conformidade com a LGPD. Disponível em: https://opiceblumacademy.com.br/wp-content/uploads/2020/02/lgpd-governanca-melhores-praticas.pdf. Acesso em 10 set. 2020.

deve-se analisar qual a extensão do dano, isolando o perímetro, certificando-se que a área violada está segura, preservando-se, dessa forma, outros sistemas. Ademais, é necessário certificar-se sobre a segurança do ambiente e, desde já, implementar novas medidas para evitar outras ameaças.

Os integrantes do comitê, por sua vez, precisam estar cientes de suas responsabilidades, além de funcionarem de forma harmônica, para que não ocorram decisões isoladas ou inviáveis aos procedimentos da empresa. No entanto, caso o dano tenha sido em grande escala, torna-se importante obter uma consultoria técnica externa, apresentando também o dano para os órgãos reguladores, as autoridades policiais e os parceiros de negócios.

Além disso, é substancial realizar a documentação de todo o processo, exemplificando a causa, como o incidente foi descoberto, bem como todos os outros dados relacionados. Ainda, recomenda-se que sejam feitas entrevistas com as pessoas envolvidas, identificação de IPs, catalogação de informações por meio de *softwares*, e avaliação dos riscos para os titulares de dados, por um pequeno núcleo de gestores e, posteriormente, a informação às autoridades e aos órgãos reguladores das jurisdições afetadas.

Logo, após o incidente de segurança, inicia-se a terceira etapa intitulada *avaliação***,** em que se pretende adotar medidas para a remediação. O objetivo principal passa a ser a incorporação de experiências e o aprimoramento de procedimentos, sendo oportuna a elaboração de um relatório final do incidente e revisão dos procedimentos. Conforme orientação da Opice Blum:

> [...] A ideia é que esse relatório apresente, ao menos: (i) o que aconteceu de fato;(ii) quais providências de preservação das evidências foram adotadas; (iii) quem integrou o comitê de crise responsável pelos trabalhos; (iv) quais foram as funções desempenhadas pelos colaboradores envolvidos; (v) quais os parceiros envolvidos e por quais motivos; (vi) os questionamentos dos titulares, da imprensa e das autoridades recebidos; (vii) as respostas apresentadas; e (viii) quais as medidas de correção técnicas e de Governança adotadas. [...][6]

O relatório será extremamente importante como meio de comprovação da atuação da organização diante do incidente, principalmente na defesa de fiscalizações e ações judiciais. Aliás, sempre se sugere que novos relatórios sejam confeccionados diante da ocorrência de novos incidentes, possibilitando uma análise da evolução dos procedimentos. Somado a isso, recomenda-se que a empresa possua um dossiê com as comprovações de seus cuidados, que

[6]BLUM, Opice. E-book: Melhores práticas de Governança e conformidade com a LGPD. Disponível em: https://opiceblumacademy.com.br/wp-content/uploads/2020/02/lgpd-governanca-melhores-praticas.pdf. Acesso em 10 set. 2020.

contenha, por exemplo, contratos com consultorias especializadas, contratos com sistemas e operadores, termos de uso, políticas de privacidade, políticas internas, atas, registros, entre outros.

Por conseguinte, os planos de resposta aos incidentes podem ser atualizados, contratos revistos, procedimentos reavaliados, além de revisão das diretrizes de notificação, dos sistemas e ferramentas de segurança. Ademais, considera-se importante a contratação prévia de um "*cyber insurance*[7]", para resguardar a organização dos prejuízos de um incidente de segurança, no entanto, isso deve ser somado às práticas de boa governança dispostas na LGPD, nos arts. 50 e 51. Em síntese, a identificação das obrigações legais ou regulatórias é elemento fundamental de qualquer plano de resposta.

De modo geral, deverá ser observada a LGPD, em consonância com as eventuais regulações setoriais a que estiverem submetidas, tais como as ISO (International Organization for Standardization), que tem vínculo intrínseco com o tema deste artigo. A ISO 27001[8] contempla requisitos para estabelecer, manter e melhorar um Sistema de Gestão de Segurança de Informação (SGSI). O SGSI preserva a confidencialidade, integridade e disponibilidade de informação, por meio de uma gestão de riscos. Logo, vê-se que a ISO 27001 está fortemente ligada à existência de um plano de resposta, que visa a mitigar riscos e proteger os dados, fornecendo confiança para as partes interessadas.

De acordo com a ISO 27001, o sistema de gestão de segurança precisa ser planejado em conformidade às necessidades da organização. O primeiro passo é verificar qual é o contexto dessa organização, isto é, definir quais são as questões internas e externas que podem afetar os resultados pretendidos do SGSI. Diante disso, deverão ser determinadas: a) as partes interessadas que são relevantes para o sistema de gestão da segurança da informação; e b) os requisitos dessas partes interessadas relevantes para a segurança da informação. Além de que, devem ser definidos os limites de aplicabilidade do SGSI.

A Direção da organização deve agir com liderança e comprometimento, assegurando que a política de segurança de informação é compatível com a direção estratégica da organização, garantindo a integração do SGSI com os processos, assegurando recursos necessários, propiciando que o sistema alcance seus resultados e comunicando a importância

[7]Seguro cibernético.
[8]ISO 27001. Disponível em: https://www.academia.edu/36980100/ABNT_NBR_ISO_IEC_27001_Tecnologia_da_informa%C3%A7%C3%A3o_T%C3%A9cnicas_de_seguran%C3%A7a_Sistemas_de_gest%C3%A3o_de_seguran%C3%A7a_da_informa%C3%A7%C3%A3o_Requisitos. Acesso em 27 set. 2021.

dessa gestão eficaz. A política de segurança de informação precisa se basear em uma tríplice: 1) estar disponível documentalmente; 2) ser comunicada dentro da organização; 3) estar disponível para as partes interessadas.

O planejamento é etapa essencial no SGSI, visto que tem por objetivo prevenir ou reduzir os efeitos indesejados, como em uma hipótese de ocorrência de um incidente de segurança. Nesse viés, a organização precisa planejar ações que considerem esses riscos e oportunidades, integrando e implementando essas medidas, dentro dos processos do SGSI e avaliando a eficácia dessas ações.

Em linhas gerais, a organização deve definir e aplicar um processo de avaliação de riscos de segurança de informação, no qual estabeleça critérios de aceitação do risco e critérios para o desempenho das avaliações dos incidentes. Além disso, deve assegurar contínuas avaliações, comparando resultados, identificando os riscos, os níveis e os responsáveis por estes; reter informações documentadas sobre o processo de avaliação de risco de segurança da informação; definir e aplicar um processo de tratamento dos riscos, selecionando as opções e determinando todos os controles necessários para a implementação daquelas que forem escolhidas; elaborar uma declaração de aplicabilidade que contenha os controles necessários e a justificativa para inclusões e obter a aprovação dos responsáveis pelos riscos e a aceitação desses riscos residuais de segurança de informação.

Ademais, os objetivos da organização precisam estar claros, sendo eles consistentes com a política de segurança de informação, e ser mensuráveis, comunicados e atualizados. Em suma, deverão estar definidos no planejamento: o que será feito; quais recursos serão necessários; quem será responsável; quando estará concluído e como os resultados serão avaliados.

A comunicação é etapa essencial nesse processo e é imprescindível que seja estabelecido: o que será comunicado; quando comunicar; quem comunicar; e o processo em que a comunicação será realizada. Somado a isso, a organização deve avaliar o desempenho do SGSI, determinando o que precisa ser melhorado e quais os métodos para monitoramento, medição, análise e avaliação. Precisa também ser estabelecido quando o monitoramento será realizado e o que será medido.

Após a obtenção desses resultados, estes serão analisados pelos responsáveis, previamente estipulados. Usualmente, deverá haver a realização de uma auditoria interna, capaz de prover informações sobre o SGSI, sendo que o modo como essa auditoria se dará precisa ser previamente estipulada. A Direção da organização tem de analisar criticamente o

sistema de gestão de segurança de informação, para assegurar sua contínua adequação e eficácia, considerando resultados da avaliação dos riscos, não conformidade, ações corretivas, mudanças nas questões internas e externas e oportunidades para melhoria contínua.

O conhecimento da ISO 31000[9] também é muito importante para que se crie um plano de respostas. O gerenciamento de riscos externos e internos auxilia as organizações no estabelecimento de estratégias, no alcance de objetivos e na tomada de decisões fundamentadas. É etapa essencial da governança e liderança, contribuindo para a melhoria dos sistemas de gestão. Com base nisso, a gestão de riscos deve ser parte integrante de todas as atividades organizacionais; possuir uma abordagem estruturada e abrangente que contribua para resultados consistentes e comparáveis; ser personalizada conforme o contexto da organização; ser inclusiva, dinâmica, haja vista que os riscos podem transfigurar ou desaparecer com a própria evolução da organização e sempre em melhoria contínua.

A gestão de riscos carece de entender o contexto da organização, enraizado em fatos sociais, culturais, políticos, tecnológicos, de relacionamento, valores, estratégias, relações e compromissos contratuais. Logo, é de suma importância que aquele que tratar o dado, não faça uso de um "plano de gestão de crise" genérico, mas, sim, personalizado, conforme as necessidades reais.

É também vital que os órgãos de supervisão assegurem os papéis organizacionais e as responsabilidades. Além do mais, devem ser alocados recursos apropriados para essa gestão, com pessoas experientes, competentes, com ferramentas de organização, procedimentos documentados, SGSI e realização de constantes treinamentos.

Nesse viés, deve ser elaborado um Relatório de Impacto à Proteção de Dados Pessoais (RIPD), um documento essencial para demonstrar como os dados pessoais são coletados, tratados, utilizados e compartilhados, além de demonstrar quais são as medidas utilizadas para mitigação de riscos. Aponta-se que, segundo o inciso XVII do art. 5º da LGPD, o RIPD é uma documentação que deve ser mantida pelo Controlador dos dados pessoais, sendo que o conteúdo do RIPD é indicado pelo parágrafo único do art. 38.

Nesse sentido, inicialmente verificar-se-á quem são os agentes de tratamento e o encarregado, as necessidades de elaboração do relatório e a descrição do tratamento. Em seguida, o reconhecimento de quem são as partes interessadas, as necessidades e a proporcionalidade do relatório e da gestão, a identificação/avaliação dos riscos, a adoção das

[9]ISO 31000. Disponível em: https://gestravp.files.wordpress.com/2013/06/iso31000-gestc3a3o-de-riscos.pdf. Acesso em 27 nov. 2021.

medidas para tratar os riscos, a aprovação do relatório e, por fim, continuar mantendo a revisão deste procedimento. Certos casos específicos impõem a necessidade da elaboração de um relatório, tais como para o tratamento de dados pessoais realizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais; quando houver infração da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos (arts. 31 e 32); e a qualquer momento sob determinação da ANPD[10] (art. 38).

Além disso, a organização tem de estabelecer uma abordagem de comunicação e consulta, facilitando uma aplicação eficaz da gestão de riscos. A comunicação consiste no compartilhamento de informações com o público-alvo, e a consulta, o fornecimento de retorno pelos participantes, capaz de contribuir com as futuras decisões. Essa etapa envolve diferentes áreas de especialização para cada fase de gestão e assegura que diferentes pontos de vista sejam observados.

À vista disso, compete a organização implementar a estrutura de gestão de riscos, mediante o desenvolvimento de um plano apropriado, incluindo prazos e recursos; a identificação de onde, quando e como diferentes tipos de decisões são tomadas pela organização, e por quem; a modificação dos processos de tomada de decisão aplicáveis, onde necessário; e a garantia de que os arranjos da organização para gerenciar riscos sejam claramente compreendidos e praticados.

Posteriormente, deverão ser avaliados os procedimentos, mensurando periodicamente o desempenho dessa gestão de riscos, sempre adequando aos objetivos da organização. Caso seja necessário, precisará haver adaptações. Além disso, é imprescindível instituir um escopo, personalizando o processo de gestão de riscos, ou seja, convém definir em qual nível essa gestão se estabelece: se estratégica, operacional, de programa, projeto ou outras atividades, e planejar o que se inclui nesse plano, por exemplo as ferramentas e técnicas apropriadas para o processo de avaliação de riscos.

A organização também precisará identificar os riscos, especificamente, em comunhão com todos os colaboradores, considerando fontes tangíveis e intangíveis de risco; causas e eventos; vulnerabilidades; ameaças; mudanças no controle externo e interno; indicadores de risco emergentes; consequências e seus impactos; fatores temporais; vieses e crenças dos envolvidos, além de tudo o mais que puder ser verificado no caso concreto.

[10]Autoridade Nacional de Proteção de Dados.

A ISO IEC/27701,[11] no tópico 6 "*guidance related to iso* 27002", traz uma série de informações complementares ao tema tratado. No que se refere às políticas de segurança de informação, a ISO dispõe que organização deve produzir uma declaração sobre o apoio e o compromisso de alcançar a legislação de proteção de dados aplicável e com os termos contratuais acordados entre a organização e seus parceiros, seus subcontratados e seus terceiros aplicáveis, que devem alocar claramente as responsabilidades entre eles. Qualquer organização que processa dados, seja um controlador ou um processador, deve considerar a legislação e regulamentação de proteção de dados aplicável - no Brasil, a LGPD, durante o desenvolvimento e manutenção de políticas de segurança da informação.

Ainda, a organização deve designar um ponto de comunicação, para que o cliente possa entrar em contato acerca do processamento. Para tanto, observe-se que essa disposição da ISO IEC/27701 se encontra em consonância com os artigos 9º, inciso IV e 41, §1º da LGPD. Além disso, há necessidade de nomear uma ou mais pessoas responsáveis por desenvolvimento, implementação, manutenção, monitoramento e governança, em toda a organização e programa de privacidade, para garantir a conformidade com todas as leis e os regulamentos aplicáveis.

Outrossim, a ISO IEC/27701 dispõe expressamente sobre a necessidade de contato com as autoridades, contato com grupos de interesses especiais, se for o caso, e que a organização sempre preze pela segurança de informação na gestão de projetos. As medidas devem ser postas em prática, incluindo a conscientização de relatórios de incidentes, para garantir que a equipe esteja ciente das possíveis consequências para a organização, o membro da equipe e o principal controlador.

Como parte do processo geral de gerenciamento de incidentes de segurança da informação, a organização deve estabelecer responsabilidades e procedimentos para identificação e registro de violações. Adicionalmente, a organização deve estabelecer responsabilidades e procedimentos relacionados à notificação às partes requeridas e à divulgação às autoridades, levando em consideração a LGPD.

O relatório de eventos de segurança da informação deve: reportar pontos fracos de segurança da informação; conter avaliações e decisões sobre eventos de segurança da informação; descrever a resposta aos incidentes de segurança da informação; possuir registros tais como descrição do incidente, o período de tempo, as consequências do incidente, para

[11]ISO IEC/27701. Disponível em:<https://br1lib.org/book/11682064/7571fb?dsource=recommend. Acesso em 27.nov.2021.

quem o incidente foi relatado, as medidas tomadas para resolver o incidente e, evidentemente, qual o fato de o incidente ter resultado em indisponibilidade, perda, divulgação ou alteração de dados, para fins regulatórios e forenses.

Como parte das análises técnicas de conformidade com as políticas e os padrões de segurança, a organização deve incluir métodos de análise dessas ferramentas e desses componentes relacionados ao processamento de dados, com o monitoramento contínuo para verificar se apenas o processamento permitido está ocorrendo e com testes específicos de vulnerabilidade.

Como verificado, é indispensável a comunicação do controlador à autoridade nacional e ao titular, quanto à ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, tal como prevê o art. 48 da LGPD. Entretanto, vige uma dúvida quanto ao prazo que essa comunicação deve se dar, já que a LGPD apresentou apenas a necessidade de que esse prazo seja *razoável*, conforme se extrai do §1º. Nesse sentido, utiliza-se como parâmetro, a legislação europeia (General data protection regulation - GDPR), na qual estabelece prazo de 72 horas, embora não de forma decisiva, com o objetivo de que a investigação não seja muito extensa.

Ademais, caso o incidente de segurança apresente dano relevante aos titulares ou possa acarretar risco, a empresa controladora dos dados deve notificar a Autoridade Nacional de Proteção de Dados (ANPD). O controlador deve notificar o titular sobre o incidente de segurança, informando-lhe a possibilidade de danos ou riscos, bem como informações para mitigação dos prejuízos. Adicionalmente, os prestadores de serviço e parceiros envolvidos, diretamente, precisam ser informados, evitando-se vulnerabilidades em situação de reincidência.

Como penalidade, a LGPD prevê a publicização da infração, para obrigar a empresa a informar sobre o incidente, caso não tenha feito isso de forma espontânea e clara. Por isso, evidencia-se a importância das empresas assinarem contratos ou termos aditivos com a cláusula de que devem ser informados no caso de ações irregulares, para que não sejam responsabilizadas por omissão de terceiros. Pela mesma razão, a LGPD determina que, na atividade de tratamento de dados pessoais, na hipótese de causar dano patrimonial, moral, individual ou coletivo, existe a obrigação de repará-lo.

Caso o incidente envolva a prática de algum crime, deve-se buscar a instauração do inquérito policial, como no caso de *ransomware*, em que há o sequestro da base de dados e a

exigência de valor em contrapartida para liberação. Nesse caso, a organização apenas demonstrará que fez o que estava ao seu alcance.

4 SANÇÕES AO CONTROLADOR

O tema deste artigo tem estrita relação com as sanções administrativas previstas no art. 52 da LGPD, haja vista que estas somente serão aplicadas após procedimento administrativo, com oportunidade de ampla defesa, considerando as peculiaridades do caso concreto com previsão no §1º, das quais ressaltam-se a adoção de política de boas práticas governança, a pronta adoção de medidas corretivas e a adoção reiterada de mecanismos e procedimentos internos capazes de minimizar o dano. Assim, é de suma importância que o plano de respostas ou um sistema de gestão de riscos esteja vigente na organização, isto porque, caso a ANPD observe que o controlador previu possíveis riscos e tomou medidas para se prevenir, as sanções poderão ser reduzidas.

Desse modo, é perceptível que a LGPD sanciona gravemente aqueles que agem de má-fé e preza por considerar cada caso de maneira única, atendendo ao princípio da proporcionalidade. Em resumo, a gravidade, a boa-fé, o grau do dano e as intenções do controlador serão os pontos mais considerados para o cálculo da sanção. Acrescenta-se, ainda, que tais previsões não substituem a aplicação de sanções administrativas, civis ou penais, conforme prevê o §2º do art. 52 da LGPD.

5 BREVE COMPARATIVO À LEGISLAÇÃO E JURISPRUDÊNCIA EUROPEIA

Os principais pontos da LGPD refletem disposições do *General Data Protection Regulation*[12] (GDPR), em vigor na União Europeia (UE). Ressalta-se, entretanto, que a legislação brasileira não realizou uma cópia do modelo europeu, sendo que a LGPD se apresenta como a primeira legislação no Brasil responsável por tratar a proteção de dados com afinco.

Evidentemente, não se despreza a importância do Marco Civil da Internet (Lei n.º 12.965, 23 de abril de 2014), da Lei de Acesso a Informações Públicas (Lei n.º 12.527, de 18 de novembro de 2011) e de certas disposições do Código de Defesa do Consumidor (Lei n.º 8.078, de 11 de setembro de 1990), que, por sua vez, devem ser utilizadas, sistematicamente, com a LGPD. Além disso, é necessário ressaltar que a própria Constituição Federal de 1988, traz a temática com muitos fragmentos e de forma indireta, sendo imprescindível, considerar a

[12]Regulamento Geral sobre Privacidade de Dados.

presença do instituto do Habeas Data, disposto no Art. 5º, LXXII, que, no entanto, apenas respalda a pessoa privada.

No que diz respeito à notificação da violação dos danos, conforme mencionado, a LGPD não detalha prazo para que seja feita a notificação do vazamento, mas apenas informa que esta seja feita em prazo razoável. Em contrapartida, a GDPR prevê prazo de 72h. Ademais, a legislação brasileira determina que os indivíduos que tiveram seus dados violados devem ser notificados do incidente, o que não é requisito do regulamento europeu.

Quanto às sanções, para a GDPR, em caso de incidente de violação de dados, pode haver aplicação de multas que variam de 10 a 20 milhões de Euros ou de 2% a 4% do faturamento anual total do exercício financeiro anterior, o que for maior, sendo que a LGPD estabelece multas simples de até 2% da receita global do exercício anterior até 50 milhões de reais por violação.

Além dessas diferenças evidentes, é importante considerar que a GDPR é uma legislação que busca ser mais objetiva e direta em seus termos, ao passo que a LGPD tem cláusulas mais abertas e subjetivas, permitindo que haja interpretações diferentes, sendo imprescindível a consulta da jurisprudência e regulamentos pela ANPD (Autoridade Nacional de Proteção de Dados). A problemática maior está no fato de que a jurisprudência ainda não se vê consolidada, já que o instituto é recente.

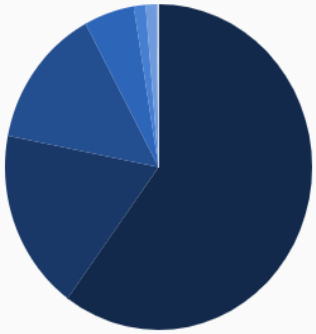
Com base em uma estatística extraída do "*CMS. Law GDPR Enforcement Tracker*[13]" em 23 de novembro de 2021, pode-se observar que a quarta maior causa de aplicação das multas pertence a "medidas técnicas e organizacionais insuficientes para garantir a segurança de informação, o que só reforça a importância da existência de um plano de respostas rápido e efetivo:

Figura 2[14]

Estatística: multas por tipo de violação

[13]Traduzido por "Rastreador de aplicação da GDPR". Disponível em: https://www.enforcementtracker.com/.
[14]GDPR Enforcement Tracker. Disponível em: https://www.enforcementtracker.com/. Acesso em 23 nov. 2021.

Pela soma total das multas:



Violação	Soma das multas
Não conformidade com os princípios gerais de processamento de dados	€ 783.975.044 (a 182 multas)
Cumprimento insuficiente de obrigações de informação	€ 234.950.395 (a 64 multas)
Base jurídica insuficiente para processamento de dados	€ 183.067.138 (a 301 multas)
Medidas técnicas e organizacionais insuficientes para garantir a segurança da informação	€ 68.993.519 (a 181 multas)
Cumprimento insuficiente dos direitos dos titulares dos dados	€ 16.321.825 (a 79 multas)
Desconhecido	€ 14.700.500 (a 4 multas)
Cumprimento insuficiente das obrigações de notificação de violação de dados	€ 1.362.091 (a 21 multas)
Acordo de processamento de dados insuficiente	€ 993.580 (a 5 multas)
Envolvimento insuficiente do oficial de proteção de dados	€ 260.200 (a 10 multas)
Cooperação insuficiente com a autoridade supervisora	€ 216.929 (a 35 multas)

Ainda, considerando que a jurisprudência brasileira é escassa no assunto, é importante contemplar algumas nuances das decisões de alguns países pertencentes à União Europeia, as quais foram obtidas pelo "Rastreador da GDPR":

Na Espanha, por exemplo, ocorreu um caso de violação ao art. 37 da GDPR, em que se verificou a ausência de nomeação de um oficial de proteção de dados (Procedimento nº: PS/ 00251/2020[15]). O artigo violado estabelece que os responsáveis pelo tratamento devem designar um "delegado" de proteção de dados. Como fatores agravantes, tem-se que o número de interessados é alto, considerando-se que é responsável por realizar o processamento de dados pessoais em grande escala, sendo que identificadores pessoais básicos foram afetados. Para tanto, foi fixada multa de € 50.000 (cinquenta mil euros). Portanto, conclui-se que, assim como a LGPD prevê a necessidade da nomeação de um DPO, a GDPR também ressalta essa informação, sendo certo que a inexistência desse importante agente, em acréscimo com os outros fatos agravantes, resultou em uma sanção de valor vultoso.

Além disso, é oportuno apresentar outro exemplo de violação da proteção de dados pessoais, retirado de um incidente ocorrido na Polônia, por violação ao art.32 da GDPR, referente à insuficiência de medidas técnicas e organizacionais para garantir a segurança de informação (Decisão: ZSOŚS.421.25.2019[16]). No caso em apreço, foi constatada uma violação na proteção de dados pessoais pela Universidade de Ciências da Vida de Varsóvia,

[15]ESPANHA. AGENCIA ESPOÑOLA PROTECCIÓN DATOS. Procedimiento Nº: PS/00251/2020. RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR. Disponível em: https://www.aepd.es/es/documento/ps-00251-2020.pdf. Acesso em 8 out. 2020.

[16]POLÔNIA. DECISÃO ZSOŚS.421.25.2019. Escritório de Proteção de Dados Pessoais. Varsóvia, 21.ago.2020. Disponível em: https://www.uodo.gov.pl/decyzje/ZSO%C5%9AS.421.25.2019. Acesso em 8 out. 2020.

devido à livre circulação de dados, tendo sido aplicada multa à Universidade no valor de 50.000 PLN (cinquenta mil PLN).

Ademais, torna-se interessante analisar um episódio ocorrido na Irlanda[17], por violação ao Art. 5 e Art. 32 da GDPR, também referente a medidas técnicas organizacionais insuficientes para garantir a segurança de informação. No caso concreto, a comissão de Proteção de Dados (DPC) aplicou uma multa de € 65.000 ao Hospital Maternidade da Universidade de Cork (CUMH) depois que os dados pessoais de 78 de seus pacientes foram descartados em uma instalação de reciclagem pública em outro lugar no condado. Sabe-se que os dados em apreço possuíam informações de natureza sensível, sendo que, se acredita que a violação envolveu dados confidenciais de saúde de pacientes, incluindo históricos médicos e futuros programas planejados de atendimento. Independentemente da razão pela qual ocorreu esse descarte indevido de dados, o hospital, como controlador de dados, foi considerado responsável. É importante frisar que o hospital informou que todos os pacientes afetados pela violação foram notificados a respeito, e a Comissão de Proteção de Dados acabou por aplicar uma multa administrativa de € 65.000.

Por fim, tendo em vista os exemplos acima extraídos da União Europeia, e diante de todos os tópicos dissertados neste artigo, verifica-se que as sanções sempre serão agravadas diante da insuficiência de medidas capazes de garantir a segurança dos dados.

6 PROPOSIÇÕES CONCLUSIVAS

Conclui-se, portanto, que a Lei Geral de Proteção de Dados é de suma importância para a regulação da vida em sociedade, no século XXI, tendo em vista o número massivo e crescente de incidentes de segurança, inviolabilidade de dados e dos diversos impactos que podem ser causados ao titular e ao controlador. Além disso, percebeu-se que a atuação preventiva contribui para a diminuição da ocorrência de incidentes, bem como minimiza, significativamente, o impacto das sanções.

De plano, restou fornecido elementos concretos para a elaboração de um plano de respostas, no qual se compõe das fases de preparação, resposta e avaliação. Em síntese, verificou-se a importância da criação de um comitê de gestão de crise, bem como a importância dos responsáveis jurídicos e do DPO. Ademais, viu-se que é imprescindível a

[17]BRENNAN, CIANAN. O hospital de Cork multou € 65.000 após os dados pessoais dos pacientes serem encontrados em uma instalação pública de reciclagem. Disponível em: https://www.irishexaminer.com/news/arid-40075673.html. Acesso em 8 out. 2020.

implementação de treinamentos, simulações de incidentes, registro das operações e o aprimoramento dos procedimentos. Conjuntamente a esses pontos, reforçou-se a necessidade de complementação do tema com as ISO's (27001; 31000; IEC/27701), as quais fornecem bases ainda mais concretas.

Outrossim, constatou-se que a adoção das políticas de boa governança está intimamente ligada à redução das sanções, visto que estas são aplicadas de acordo com as peculiaridades do caso concreto. Ainda, restou observado alguns aspectos da GDPR e jurisprudências europeias, que reforçam, sobretudo, a importância do DPO e a adoção de medidas técnicas e organizacionais para prevenir e remediar danos, em que se encontra na quarta maior causa de aplicação de multas na União Europeia.

Finalmente, entende-se que a existência de um plano de respostas é tarefa primordial que não pode ser deixada em segundo plano, sendo certo que o presente artigo não esgota o tema, o qual está em constantes atualizações.

REFERÊNCIAS BIBLIOGRÁFICAS

APÓS SANÇÃO DO GOVERNO, LEI GERAL DE PROTEÇÃO DE DADOS COMEÇA A VALER. **Consultor jurídico**, 2020. Disponível em: https://www.conjur.com.br/2020-set-18/sancao-governo-lgpd-comeca-valer-nesta-sexta. Acesso em: 10 out. 2020.

AS FUNÇÕES DO DPO DE ACORDO COM A GDPR. **Assis e Mendes Advogados**, 2020. Disponível em: https://assisemendes.com.br/funcoes-dpo/. Acesso em: 19 nov.2021.

BANCO INTER CONFIRMA VAZAMENTO DE DADOS E CULPA PESSOA AUTORIZADA. **UOL**, 2020. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2018/08/17/banco-inter-confirma-vazamento-de-dados-apos-ataque-hacker.htm. Acesso em: 15 set. 2020.

BLUM, Renato Opice. Plano de resposta a incidentes de segurança de dados pessoais: uma prevenção importante. **Opce blum**, 2020. Disponível em: https://noomis.febraban.org.br/especialista/renato-opice-blum/plano-de-resposta-a-incidentes-de-seguranca-de-dados-pessoais-uma-prevencao-importante. Acesso em: 26 ago. 2020.

BRASIL. **Lei Geral de Proteção de Dados (LGPD) nº 13.709**, de 14 de agosto de 2018. Diário Oficial, Brasília, 14 de agosto de 2018.

BRASIL. Apelação Cível 1006311-89.2020.8.26.0001**.** Tribunal de Justiça do Estado de São Paulo. Relatora Maria Lúcia Pizzotti. 30ª Câmara de Direito Privado. Foro Regional I - Santana, 8ª Vara Cível. **Tjsp,** 01/09/2021. Disponível em: https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=14982708&cdForo=0. Acesso em: 24 nov. 2021.

BRAZ, Marcilio. Considerações sobre a notificação de incidentes de segurança da informação no contexto da lei geral de proteção de dados. **Migalhas**, 2020. Disponível em: https://www.migalhas.com.br/depeso/295440/consideracoes-sobre-a-notificacao-de-incidente-de-seguranca-da-informacao-no-contexto-da-lei-geral-de-protecao-de-dados-e-alem#:~:text=Art.,ou%20dano%20relevante%20aos%20titulares.&text=VI%20%2D%20as%20medidas%20que%20foram,mitigar%20os%20efeitos%20do%20preju%C3%ADzo>. Acesso em: 22 set. 2020.

BRENNAN, Cianan. O hospital de Cork multou € 65.000 após os dados pessoais dos pacientes serem encontrados em uma instalação pública de reciclagem**. Irish examiner**, 2020. Disponível em: https://www.irishexaminer.com/news/arid-40075673.html. Acesso em: 8 out. 2020.

BRUNO, M.; VAINSOF, R. et al. Melhores práticas de Governança e conformidade com a LGPD. São Paulo: **Opce blum**. E-book: Disponível em: https://opiceblumacademy.com.br/wp-content/uploads/2020/02/lgpd-governanca-melhores-praticas.pdf. Acesso em: 10 set. 2020.

DECISÃO ZSOŚS.421.25.2019. **Escritório de Proteção de Dados Pessoais. Polônia, Varsóvia**, 21.ago.2020. Disponível em: https://www.uodo.gov.pl/decyzje/ZSO%C5%9AS.421.25.2019. Acesso em: 8 out.2020.

DPO: UM NOVO CARGO EXIGIDO PELA LGPD**. Delphos**. Disponível em: https://www.delphos.com.br/dpo-e-lgpd/. Acesso em: 19 nov. 2021.

EFEITOS E PROJEÇÕES SOBRE A VIGÊNCIA DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E O PAPEL DO ENCARREGADO DOS DADOS PESSOAIS**. Contecsi.** Disponível em: http://contecsi.submissao.com.br/arquivos/6598.pdf. Acesso em: 13 out. 2020.

É PRECISO APRENDER A LIDAR COM INCIDENTE DE DADOS. **SERPRO**. Disponível em: https://www.serpro.gov.br/lgpd/noticias/2020/aprender-lidar-indicendes-dados-lgpd. Acesso em: 26 ago. 2020.

GDPR ENFORCEMENT TRACKER**. Enforcementtracker.** Disponível em: https://www.enforcementtracker.com/. Acesso em: 23 nov. 2021.

GUIA LGPD GOVERNANÇA DE DADOS**.** Brasília, DF: Presidência da República. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf. Acesso em: 28 set. 2020.

GESTÃO DE INCIDENTES DE SEGURANÇA DE INFORMAÇÃO. **IBLISS, Digital Security.** Disponível em: https://www.ibliss.digital/gestao-de-incidentes-de-seguranca-da-informacao/. Acesso em: 26 ago.2020.

HERRERO, Vagner Henrique. A lei de proteção de dados pessoais brasileira e os desafios a esta administração pública**. Repositório Institucional Universidade Federal de Minas Gerais**, 2019. Disponível em: https://repositorio.ufmg.br/bitstream/1843/32044/1/VagnerHenriqueHerrero.pdf. Acesso em: 10 set. 2020.

INCIDENTES DE SEGURANÇA DA INFORMAÇÃO. **Superintendência de Tecnologia da Informação e Comunicação - UFRJ.** Disponível em: https://www.security.ufrj.br/denuncie-um-incidente/. Acesso em: 26 ago. 2020.

ISO 27001**. Academia.edu**, 2021. Disponível em: https://www.academia.edu/36980100/ABNT_NBR_ISO_IEC_27001_Tecnologia_da_informa%C3%A7%C3%A3o_T%C3%A9cnicas_de_seguran%C3%A7a_Sistemas_de_gest%C3%A3o_de_seguran%C3%A7a_da_informa%C3%A7%C3%A3o_Requisitos. Acesso em: 27 nov.2021.

ISO 31000. **Gestravp**, 2013. Disponível em: https://gestravp.files.wordpress.com/2013/06/iso31000-gestc3a3o-de-riscos.pdf. Acesso em: 27 nov. 2021.

ISO IEC/27701. **Br1lib**. Disponível em: https://br1lib.org/book/11682064/7571fb?dsource=recommend. Acesso em: 27 nov.2021.

KOHN, Stephanie. Maior ataque da história estremece a internet. **Olhar digital.** Disponível em: https://olhardigital.com.br/fique_seguro/noticia/maior-ataque-cibernetico-da-historia-estremece-a-internet/33511. Acesso em: 26 ago.2020.

LGPD X GDPR: QUAIS AS SEMELHANÇAS E DIFERENÇAS. **Alleasy.** Disponível em: https://www.alleasy.com.br/2020/03/09/lgpd-x-gdpr-semelhancas-diferencas/#:~:text=A%20LGPD%20n%C3%A3o%20possui%20prazos,notificados%20dentro%20de%2072%20horas. Acesso em: 28 set.2020.

MACHADO, José Mauro Decoussau *et al.* LGPD e GDPR: Uma análise comparativa entre as legislações. **Pinheiro Neto Advogados**, 2018. Disponível em: http://www.pinheironeto.com.br/publicacoes/lgpd-e-gdpr-uma-analise-comparativa-entre-as-legislacoes. Acesso em: 28 set. 2020.

MASSENO, Manuel David. A segurança dos dados na LGPD, brasileira: Uma perspectiva europeia, desde Portugal. **Revista do Direito**. Santa Cruz do Sul, v. 3, n. 50, p. 80-103, jan./abr. 2020. Disponível em: https://online.unisc.br/seer/index.php/direito/index.

NETO, Thaís. Aplicação de Sanções Administrativas na LGPD – Lei Geral de Proteção de Dados**. Instituto de Diretório Real**, 2020. Disponível em: https://direitoreal.com.br/artigos/aplicacao-de-sancoes-administrativas-na-lgpd-lei-geral-de-protecao-de-dados. Acesso em: 10 out.2020.

NUNES, Natália Martins. LGPD: Como as startups devem se preparar para casos de incidentes de segurança. **Jusbrasil**, 2020. Disponível em: https://ndmadvogados.jusbrasil.com.br/artigos/853810779/lgpd-como-as-startups-devem-se-preparar-para-casos-de-incidentes-de-seguranca?ref=feed. Acesso em: 10 set. 2020.

O QUE ESTÃO FAZENDO COM OS MEUS DADOS? A IMPORTÂNCIA DA LEI GERAL DE PROTEÇÃO DE DADOS. Coordenação: Paloma Mendes Saldanha. Recife:

SerifaFina, 2019. **Udop.** Disponível em: https://apphotspot.com.br/wp-content/uploads/elementor/forms/OAB-PE-Oque-est%C3%A3o-fazendo-com-meus-dados-LGPD.pdf.

PALMA, Fernando. Incidentes de Segurança da Informação: conceitos, exemplos e cases. **Portalgsti**, 2014. Disponível em: https://www.portalgsti.com.br/2014/01/incidentes-de-seguranca-da-informacao-conceito-exemplos-e-cases.html. Acesso em: 26 ago.2020.

POR QUE DEVO REPORTAR INCIDENTES? **Pró-reitora de Gestão da Informação e Comunicação da UFPEL**. Disponível em: https://wp.ufpel.edu.br/seginfo/reportar-incidente-de-seguranca/. Acesso em: 22 set. 2020.

PROCEDIMIENTO Nº: PS/00251/2020 RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR. Espanha. **Agencia Espoñola Protección Datos**. Disponível em: https://www.aepd.es/es/documento/ps-00251-2020.pdf. Acesso em: 8 out.2020.

RODAS, Sérgio. Senado aprova vigência imediata da LGPD, mas prazo depende de sanção. **Consultor jurídico**. Disponível em: https://www.conjur.com.br/2020-ago-26/lei-geral-protecao-dados-vigencia-imediata-senado. Acesso em: 10 out. 2020.

SOMBRA, Thiago Luís; CASTELLANO, Ana Carolina. Plano de Resposta a Incidentes de Segurança: reagindo rápido e de forma efetiva. **Revista do Advogado.** AASP, 2019. v. 39, n. 144, nov, p. 168-173.

TECNOLOGIA E DA INFORMAÇÃO/OAB-PE. **Udop**. Disponível em: https://www.udop.com.br/download/noticias/2020/03_03_20_arquivo_oab_pe.pdf#page=19. Acesso em: 13 out. 2020.

VOCÊ SABE O QUE É RESPOSTA A INCIDENTES DE SEGURANÇA? **Real protect**. Disponível em: https://realprotect.net/blog/voce-sabe-o-que-e-resposta-incidentes-de-seguranca/. Acesso em: 15 set. 2020.

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS NA LEI GERAL DE PROTEÇÃO DE DADOS: UMA BANALIZAÇÃO?

PERSONAL DATA PROTECTION IMPACT REPORT (RIPD) IN BRAZILIAN GENERAL DATA PROTECTION LAW: A BANALIZATION?

IAN MATIELLO GRASSO[1]

SUMÁRIO: 1. INTRODUÇÃO. 2. A VIRADA REGULATÓRIA. 3. BREVE HISTÓRICO DAS FERRAMENTAS. 4. CONCLUSÕES. BIBLIOGRAFIA.

RESUMO

Este artigo tem como objetivo estudar o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) a partir de seus predecessores: as *impact assessments*, o *Privacy Impact Assessment*, do Reino Unido, e o *Data Protection Impact Assessment (DPIA), do General Data Protection Regulation (GDPR)*, analisando a experiência europeia sobre o tema, bem como de que modo a regulação brasileira o incorporou, explorando possíveis problemas e soluções.

Palavras-chave: Direito Digital; Lei Geral de Proteção de Dados; Relatório de Impacto à Proteção de Dados Pessoais (RIPD).

ABSTRACT

This article aims to study the Personal Data Protection Impact Report (RIPD) from its predecessors: as impact assessments, the UK Privacy Impact Assessment and the Data Protection Impact Assessment (DPIA) of the General Data Protection Regulation (GDPR), analyzing the European experience on the subject, as well as how Brazilian regulation incorporated it, exploring possible problems and solutions.

Keywords: Digital Law; Brazilian General Data Protection Law; Personal Data Protection Impact Report (RIPD).

1 INTRODUÇÃO

[1] Graduando em Direito pela Faculdade de Direito de Sorocaba. Artigo Científico apresentado como resultado dos trabalhos realizados no Grupo de Estudos em Direito Digital da Faculdade de Direito de Sorocaba (2020-2021). E-mail. ian.m.grasso@hotmail.com.

A Lei 13.709/18 (Lei Geral de Proteção de Dados Pessoais), em vigor desde 18/09/2020, tornou-se, no ordenamento jurídico pátrio, a peça central na sistemática de proteção aos direitos de privacidade e dos titulares de dados pessoais. A abordagem regulatória trazida pela LGPD é parte de um novo capítulo no mundo jurídico, o da "risquificação" dos direitos, "onde a afirmação de direitos fundamentais é complementada por uma preocupação maior com instrumentos de regulação *ex ante*, licenças, análises de risco, processos de documentação e accountability por parte dos 'controladores' e 'processadores' de dados (GELLERT, 2015; QUELLE, 2015; SPINA, 2017).[2]'

Nesta perspectiva, para operacionalizar seus ditames na rotina das organizações, "a LGPD pode ser encarada como uma 'caixa de ferramentas' (BENNETT; RAAB, 2006), na qual vão existir obrigações que servem como instrumentos e conceitos que nos ensinam a como manusear essas ferramentas de forma adequada e eficiente[3]".

A base teórica da lei geral brasileira foi inspirada fortemente pela experiência europeia de elaboração do *General Data Protection Regulation (GDPR)*, com adaptações pelo legislador nacional, trazendo diversas obrigações e instrumentos semelhantes entre si, e entre eles, o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), equivalente ao *Data Protection Impact Assessment (DPIA)* europeu.

A ferramenta foi pensada e moldada com a função de desempenhar papel central na sistemática de proteção de dados do bloco europeu[4]. Assim sendo, "errar a mão" em sua regulação tem duas consequências principais que serão catastróficas: desperdiçará e dissipará os esforços da Autoridade Nacional de Proteção de Dados (ANPD) e onerará excessivamente os controladores e operadores com uma possível obrigação legal meramente formal, o que vai na contramão da sistemática preventiva trazida pelo *GDPR* e pela LGPD.

Até o momento, permanece o cenário de incertezas de como o tema será abordado pela Autoridade Nacional, e os desafios para a regulação do RIPD não são poucos, principalmente por conta da incompreensão da ferramenta. Pra tanto, Maria Cecilia Oliveira Gomes mapeou

[2] ZANATTA, Rafael A.F. *"PROTEÇÃO DE DADOS PESSOAIS COMO REGULAÇÃO DE RISCO: uma nova moldura teórica?"* (2017). Artigos Selecionados REDE 2017. I Encontro da Rede de Pesquisa em Governança da Internet. p. 176.

[3] GOMES**,** Maria Cecília Oliveira. *Relatório de Impacto a Proteção de Dados Pessoais: uma breve análise da sua definição e papel na LGPD* (2019), Revista da AASP, n. 144. p. 07.

[4] Kloza, Dariusz & Dijk, Niels & Gellert, Raphaël & Böröcz, István & Tanas, Alessia & Mantovani, Eugenio & Quinn, Paul. (2017). *Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals***.** p. 01.

os principais desafios para a regulação do RIPD brasileiro, sugerindo cinco eixos de análise: (i) identificar o que é a ferramenta, as reais funções do relatório e seu papel dentro da LGPD; (ii) a noção de risco e a sua análise e documentação; (iii) as hipóteses de obrigatoriedade de elaboração; (iv) a metodologia adequada para elaboração do relatório; e (v) o estabelecimento de parâmetros para demonstrar a prestação de contas à ANPD, bem como sua eventual publicização.[5]

Tecidas estas breves considerações, o presente artigo científico visa contribuir com o debate nacional acerca do tema, e para isso, buscar-se compreender o que é o relatório, suas reais funções e finalidades, a partir do pano de fundo teórico da abordagens *rights-based* e *risk-based*, traçando um histórico dos predecessores desta ferramenta, começando com as *impact assessments*, com o *Privacy Impact Assessment* nos moldes dados pelo *Information Comissioneer's Office (ICO)* e com o *Data Protection Impact Assessment (DPIA)* do *General Data Protecion Regulation (GDPR)* da União Europeia, que culminou no nosso Relatório de Impacto à Proteção de Dados (RIPD).

2 A VIRADA REGULATÓRIA

O pano de fundo teórico em que esses tipos de ferramentas se originaram é o debate acerca das abordagens regulatórias baseadas nos direitos fundamentais (*rights-based approach)* e no risco (risk-based approach). A compreensão disso é fundamental para a compreensão da ferramenta.

Autores como Rafael F. A. Zanatta entendem que não há uma dicotomia propriamente dita entre as abordagens *rights-based* e *risk-based* nessa "guinada teórica[6]", mas sim uma "fricção" entre elas, em que a sistemática de avaliação de riscos é incorporada no modelo teórico da proteção dos direitos fundamentais. Todavia, a risquificação da proteção jurídica aos

[5] GOMES, Maria Cecília Oliveira. *Desafios da Regulamentação do Relatório de Impacto (2021)*. Disponível em https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/desafios-da-regulamentacao-do-relatorio-de-impacto-11022021. p. 04.

[6] Zanatta entende por "guinada teórica" justamente esse processo de incorporação do modelo baseado em risco ao modelo regulatório dos direitos fundamentais no debate da proteção de dados pessoais.

direitos fundamentais pode ser fragilizada consideravelmente quando a abordagem baseada em riscos é incorretamente incorporada ou aplicada.[7]

O debate da fricção entre os modelos teóricos é rico e atual. A título de exemplo, a ONG *Access Now*, cujo foco é a defesa dos direitos civis digitais, em resposta à consulta pública da proposta de regulamentação em aplicações que usam inteligência artificial do parlamento europeu, criticou fortemente a abordagem baseada em riscos quando aplicada a regulação de aplicações que utilizam de Inteligência Artificial.

As críticas principais foram que o *GDPR* não é uma regulamentação baseada em risco, e que os pontos do regulamento geral europeu, em que predominam a análise de risco, revelaram-se problemáticos por diversos fatores[8], destacando-se o caráter altamente imprevisível que sistemas de inteligência artificial podem tomar se pertencentes a uma "zona cinzenta" nas avaliações de risco. Então, um sistema, cujas consequências aos titulares são altamente imprevisíveis, pode ser classificado pela autoridade de *enforcement* ou pelo controlador como de baixo-risco, e por consequência, são desnecessárias medidas adicionais de mitigação desses riscos, o que pode gerar consequências catastróficas ou uma violação direta aos direitos e liberdades fundamentais dos titulares.

Outro ponto interessante destacado foi o de que uma iniciativa que utilize de I.A. pode ser frontalmente contrária aos direitos do titular e à legislação, e mesmo assim, ser implementada e utilizada, confundindo o que é violação direta (ou *non-compliance)* com risco, relegando a sua análise para uma fase posterior da avaliação de impacto, o que medida nenhuma de mitigação pode corrigir ou remediar, situação esta que enfraquece os mecanismos de prevenção e proteção aos titulares como um todo. [9]

Esse tipo de confusão ocorreu no cenário regulatório europeu, cujos agentes, como os órgãos de governo e a sociedade civil, possuíam considerável maturidade atinente ao tema de proteção de dados, levando em consideração a Diretiva 95/46/EC, vigente desde 1998, sem

[7] ZANATTA, Rafael A.F. *PROTEÇÃO DE DADOS PESSOAIS COMO REGULAÇÃO DE RISCO: uma nova moldura teórica?* (2017). Artigos Selecionados REDE 2017. I Encontro da Rede de Pesquisa em Governança da Internet. p. 176.

[8] As avaliações de risco no GDPR ocorrem tipicamente na elaboração do DPIA e quando há incidentes de segurança.

[9] Access Now. *The EU should regulate AI on the basis of rights, not risks***.** 17 de fevereiro de 2021. Disponível em: https://www.accessnow.org/eu-regulation-ai-risk-based-approach/.

contar com as diversas leis nacionais dos estados-membros, cujas origens datam da década de 1970.

A confusão consistia no crescente entendimento equivocado de que as abordagens baseadas em risco seriam uma substituição ao modelo baseado nos direitos de proteção de dados pessoais e de seus princípios.

Para tanto, a *Working Party 29* (WP29), em 30 de maio de 2014, emitiu um parecer técnico sobre a função das abordagens em risco no *framework* regulatório de proteção de dados pessoais, visando esclarecer tal problemática e as questões levantadas pelos vigorosos debates da época.

Nessa esteira, o ponto fulcral das ferramentas *risk-based* é o de que estas têm como função uma abordagem *escalável e proporcional ao compliance*, isto é, para o controlador, cujas atividades de processamento de dados são de baixo risco, não há necessidade de fazer tanto para se adequar[10] às suas obrigações legais quanto um controlador cujo processamento tenha alto risco.[11]

As obrigações de adequação à lei dos controladores e operadores permanecem as mesmas, principalmente no tocante aos direitos do titular (como os direitos de acesso, portabilidade dos dados, etc.) e aos princípios do GDPR, independente do risco do processamento. O que pode sofrer alterações é justamente a obrigação de demonstração (incluídas as de documentação e de medidas adicionais de mitigação de risco) desse *compliance*.

Quanto aos princípios aplicáveis aos controladores, permanecem os mesmos, independentemente dos riscos do processamento. Todavia, a WP29 faz uma ressalva:

> "Os princípios fundamentais aplicáveis aos controladores (ou seja, legitimidade, minimização dos dados, limitação da finalidade, transparência, integridade dos dados, precisão dos dados) devem permanecer os mesmos, independentemente do processamento e dos riscos para os titulares dos dados. No entanto, a devida consideração à natureza e ao escopo de tal processamento sempre foram parte integrante da aplicação desses princípios, de modo que eles são inerentemente escaláveis"[12]

[10] E por consequência lógica, comprovar sua adequação, em atenção ao princípio do *accountability.*

11 WP29, *"Statement of the WP29 on the role of a risk-based approach in data protection legal frameworks"* (2014). p. 2.

[12] "Fundamental principles applicable to the controllers (i.e. legitimacy, data minimization, purpose limitation, transparency, data integrity, data accuracy) should remain the same, whatever the processing and the risks for the data subjects. However, due regard to the nature and scope of such processing have always been an integral part of the application of those principles, so that they are inherently scalable". Ibidem. p.3.

A WP29 traz a presença dos vocábulos "adequado", "apropriado", "razoável" e "necessário" dos artigos 6º e 7º, da Diretiva 95/46/EC. Por exemplo, o juízo de adequação de necessidade ou de razoabilidade do tratamento de dados, com as finalidades almejadas, é inerente a tais princípios, e nenhum controlador pode furtar-se de observá-los. Aqui, o elemento "risco" não é determinante para a aplicação correta dos princípios ao caso concreto. Todavia:

> "as obrigações dos controladores por meio de ferramentas e medidas de responsabilidade (por exemplo, avaliação de impacto, proteção de dados desde o projeto, notificação de violação de dados, medidas de segurança, certificações) podem e devem ser variadas de acordo com o tipo de processamento e os riscos de privacidade para os titulares dos dados. O que pode variar, entretanto, é o nível de obrigações de prestação de contas, que dependerá do risco da atividade." (tradução livre)[13]

Tanto na sistemática da Diretiva 95/46/EC, do *GDPR* e da LGPD, a obrigação de documentar as atividades de processamento e de implementar medidas de segurança mínimas para resguardar os direitos do titular são gerais e indistintas,[14] independente do alto ou baixo risco da operação, mas há obrigações específicas que são desencadeadas em momentos específicos. A régua escolhida pela Diretiva e pelo *GDPR*, que determina essa escalabilidade de obrigações para os agentes de tratamento, é o fator "alto risco ao titular".

O que pode variar é a *forma* com que estes riscos são identificados, avaliados, mitigados e documentados, e a *forma* escolhida pela lei é, para tanto, uma avaliação de impacto, gênero no qual o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), o DPIA e o PIA são espécies.

Então, sob a égide da proteção de dados pessoais dos indivíduos e de seus direitos e liberdades fundamentais, não basta somente uma dicotomia purista de modelos regulatórios. Tampouco basta a pura e simples incorporação de elementos de risco nas legislações, principalmente em proteção de dados. É preciso delimitar bem as bases teóricas e premissas nas quais estas avaliações de riscos são fundadas, não somente para fins de esclarecimento e correta aplicação de tais ferramentas pelos controladores, mas para a eficácia máxima de todo o sistema.

---

[13] Ibidem. p.3.

[14] Dialogando com a LGPD, isso pode ser extraído dos princípios da segurança, da prevenção e da responsabilização e prestação de contas (art. 6º, incisos VII, VIII e X) e do art. 46, caput, da lei, sem prejuízo de o.tros: "Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".

3 BREVE HISTÓRICO DAS FERRAMENTAS

a) As *Impact Assessments* (Avaliações de Impacto)

As *Impact Assessments* surgiram nessa virada regulatória mundial, que saiu da órbita predominantemente fiscalizatória e repressiva para uma concentração de esforços por parte dos órgãos competentes e dos agentes econômicos em evitar ao máximo que ocorra o evento danoso, seja ambiental, nuclear, biotecnológico ou em proteção de dados.

As *Impact Assessments (IA)* podem ser definidas como:

> "um processo estruturado para considerar as implicações, para as pessoas e seu ambiente, das ações propostas, enquanto ainda há uma oportunidade de modificá-las (ou mesmo, se for o caso, abandoná-las). É aplicado em todos os níveis de tomada de decisão, desde políticas a projetos específicos"[15].

Roger Clarke as sistematizou e classificou de acordo com o enfoque que dão[16]:

> **Foco em tecnologia**
>
> ● *Technology* (Impact) *Assessment* (TA) – Avaliação de Impacto Tecnológico. Foca em uma tecnologia em geral. Ex. Identificação por radiofrequência (RFID), inteligência artificial, *machine learning*, medidores *smart*, drones, blockchain, etc.
>
> **Foco em projetos**
>
> ● *Technology Application Impact* Assessment – Avaliação de Impacto à Aplicação Tecnológica.
> Foca no uso específico de uma tecnologia ou mais, combinada com processo (ou método) de negócio e/ou disposições regulatórias. Ex. Identificação RFID em roupas, Inteligência Artificial em reconhecimento de linguagens, medidores *smart* em eletrodomésticos, drones para uso policial, etc.
> ● *Security Impact Assessment* / *Threat Risk Assessment* (TRA) – Avaliação de Impacto à Segurança ou Avaliação de Riscos de Ameaças.
> Foca nos impactos ou nos riscos em segurança de ativos.
>
> **Foco em impacto social**
>
> ● *Social Impact Assessment* – Avaliação de Impacto Social
> Foca nos impactos a valores sociais
> ○ *Rights Impact Assessment* – Avaliação de Impacto à Direitos Fundamentais
> Foca nos impactos aos direitos humanos, fundamentais e liberdades civis.
> ○ *Ethical Impact Assessment* – Avaliação de Impacto Ético
> Foca nos problemas ou dilemas éticos surgidos com o desenvolvimento de novas tecnologias.
> ● *Surveillance Impact Assessment* – Avaliação de Impacto à Vigilância[17]
> Foca nos impactos das tecnologias de vigilância nas múltiplas dimensões da privacidade.

[15] "Impact assessment (IA) is a structured process for considering the implications, for people and their environment, of proposed actions while there is still an opportunity to modify (or even, if appropriate, abandon) the proposals. It is applied at all levels of decision-making, from policies to specific projects". Disponível em: https://www.iaia.org/wiki-details.php?ID=4.

[16] CLARKE, Roger. *Approaches to Impact Assessment (2014). Exhibit 1: Assessment Categories***.** According to Focus. Disponível em: http://www.rogerclarke.com/SOS/IA-1401.html#AF.

[17] Interessante ressaltar que esta avaliação está prevista no anteprojeto da Lei de Proteção de Dados para segurança pública e persecução penal, batizado de LGPD Penal.

> ● *Privacy Impact Assessment* (PIA) – Avaliação de Impacto à Privacidade
> Foca nos impactos em todas as dimensões da privacidade.
> ● *Data Privacy Impact Assessment* (DPIA - Tipo 1) – Avaliação de Impacto à Privacidade Informacional
> Foca nos impactos na dimensão de privacidade informacional (*data privacy*/*information privacy)*
>
> **Foco em Compliance**
>
> ● *Regulatory Compliance*
> Foca na adequação/conformidade de uma proposta ou prática com todas as normas relevantes:
> ○ Instrumentos auto-regulatórios organizacionais. Ex. Códigos de Ética.
> ○ Instrumentos auto-regulatórios da indústria. Ex. Códigos de prática da indústria, padrões internacionais de processos e técnicas.
> ○ Instrumentos co-regulatórios. Ex. Os códigos de boas práticas previstos no art. 50 da LGPD; e
> ○ Instrumentos regulatórios formais.[18]
> ● *Legal Compliance*
> Foca na adequação de uma proposta ou prática perante todas as leis relevantes:
> ○ *Privacy Law Compliance*, i.e. adequação com todas as normas jurídicas e jurisprudência dominante que envolvam o direito à privacidade.
> ○ *Data Privacy Law Compliance*, i.e. adequação com todas as normas jurídicas e jurisprudência dominante que regulem a dimensão de *data privacy*.
> ● Statutory Compliance
> Foca na adequação de uma proposta ou prática com uma parte específica da legislação:
> ○ *Data Protection Impact Assessment* (DPIA - Type 2)
> Foca na adequação de uma proposta ou prática com o *GDPR* ou o seu equivalente em cada estado membro da UE.

O traço distintivo das *impact assessments* como gênero é a deflagração da ferramenta quando o projeto pode ser modificado substancialmente, apoiando a tomada de decisão dos envolvidos. Já como espécies, as avaliações se diferenciam de acordo com o enfoque ou escopo. Todavia, para o presente artigo, serão analisadas apenas três espécies das avaliações de impacto: *Privacy Impact Assessment (PIA), Data Privacy Impact Assessment (DPIA – Tipo 1), e Data Protection Impact Assessment (DPIA – Tipo 2).*

Como se vê, o foco do PIA é a privacidade do indivíduo, considerada em todas as suas dimensões sociais possíveis, questão essa que não depende *a priori* de proteção normativa; o *Data Privacy Impact Assessment* (DPIA – tipo 1) considera a privacidade informacional, escopo reduzido ao PIA; já o *Data Protection Impact Assessment (DPIA – tipo 2)*, o instrumento previsto no *GDPR* é classificado como uma avaliação com foco na adequação regulatória

[18] Entendo que esta subclassificação específica não se aplica ao direito brasileiro por se tratar da tradição da *civil law* e não da *common law*, razão pela qual os termos *regulatory compliance*, *legal compliance* e *statutory compliance* não serão traduzidos.

de apenas um diploma legal em específico, ou seja, considera os pontos da privacidade informacional que o *GDPR* regulamenta.

A diferenciação do enfoque de avaliação da ferramenta pode parecer apenas acadêmica, mas é crucial para definir os limites da obrigação do controlador, e, portanto, o que pode e o que não pode ser exigido pela autoridade nacional competente.

b) Os precursores do *Privacy Impact Assessment* (PIA) e a sua relação com a Diretiva 95/46/EC

O PIA começou a ser amplamente utilizado por volta da década de noventa[19] em várias jurisdições do globo, mas seu surgimento data suas raízes por volta de 1970.

Os seus precursores diretos foram a ideia de *technology assessment*, utilizada pelo *Office of Technology Assessment (OTA)*, órgão auxiliar do Congresso norte-americano, desde a sua criação (1972) até seu desmantelamento (1995). Apesar de sua extinção nos EUA, este exemplo foi seguido pela Europa, que criou a *European Parliamentary Technology Assessment (EPTA)*, criado em 1990, que permanece na ativa até os dias atuais.

O objetivo desses órgãos, por consequência do relatório elaborado por eles, é avaliar as consequências sociais do uso de certas tecnologias e ciências, apoiando a decisão dos parlamentares.[20] Outros precursores, talvez os mais conhecidos, foram os *Environmental Impact Statements (EIS)* e *Environmental Impact Assessment (EIA)*, sendo este último focado em avaliar as consequências de um projeto da perspectiva ambiental (CLARKE, 2009). Na Europa, já no campo das primeiras leis de proteção de dados do continente, deve-se notar como precursores do PIA os *pre-decisional assessments*, algo como *compliance checking* das leis, e a sistemática de checagem prévia da Diretiva 95/46/CE.[21]

A Diretiva foi a primeira norma geral da União Europeia que regulava a Proteção de Dados Pessoais do bloco, e visava precipuamente favorecer e proteger o livre fluxo de dados dentro da União, os direitos e as liberdades fundamentais dos cidadãos europeus, notadamente o direito à vida privada, considerando as divergências normativas constantes entre legislações

[19] CLARKE, Roger. *An evaluation of privacy impact Assessment guidance documents* (2011), International Data Privacy Law, 2011, Vol. 1, No. 2, p. 111.
[20] Disponível em: https://eptanetwork.org/about/about-epta.
[21] CLARKE, Roger. *Privacy Impact Assessment: Its Origins and Development*, Roger Clarke, Computer Law & Security Review 25, 2 (2009), pgs. 123-135.

nacionais de proteção de dados dos estados membros, e a positivação dos direitos à privacidade e autodeterminação informativa na Carta dos Direitos da UE.

Nos artigos 18 a 20 da Diretiva, o diploma inaugurou a sistemática de notificação e checagem prévia às respectivas Autoridades Nacionais de Proteção de Dados de cada estado membro. Nessa sistemática, a regra geral era que o controlador deveria notificar a autoridade nacional antes de realizar qualquer tratamento de dados total ou parcialmente automatizada, ou o conjunto destas operações, realizados para uma única finalidade ou finalidades semelhantes.

Esta notificação deveria conter, no mínimo: o nome e o endereço do responsável pelo tratamento e, eventualmente, do seu representante; as finalidades do tratamento; a descrição das categorias de pessoas em causa e dos dados ou categorias de dados que lhes respeitem; os destinatários ou categorias de destinatários a quem os dados poderão ser comunicados; as transferências de dados previstas para países terceiros; a descrição geral que permita avaliar de forma preliminar a adequação das medidas tomadas para garantir a segurança do tratamento em aplicação do artigo 17[22].

Todavia, os estados membros poderiam dispensar essa obrigação de notificação ou estabelecer uma notificação simplificada, exceções estas relacionadas com atividades de processamento de baixo risco e com a presença do encarregado, nas seguintes hipóteses:

> "2. Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:
> - where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored, and/or:
> - where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:
> - for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive.
> - for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2),

[22] Este artigo estabelecia obrigações operacionais mínimas ao controlador para tratamento de dados realizado, sendo a principal delas o dever de pôr em prática medidas técnicas e organizacionais adequadas para proteger os dados pessoais contra a destruição acidental ou ilícita, a perda acidental, a alteração, a difusão ou acesso não autorizados, principalmente quando os dados tratados forem transmitidos via rede, e contra qualquer outra forma de tratamento ilícito.

> thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations."[23]

Ao receber a notificação, ou quando a autoridade fosse consultada pelo encarregado de proteção de dados do controlador, ao verificar que a atividade ali descrita apresentava "riscos específicos" aos direitos e liberdades dos indivíduos, procede-se a checagem prévia, analisando tal atividade detalhadamente e autorizando ou não o seu prosseguimento.

Contudo, a sistemática de notificação geral e checagem prévia *(prior checking)* era ineficaz ao objetivo último da Diretiva, o que culminou no seu abandono, com a promulgação do *General Data Protection Regulation* (GDPR), o que será explorado futuramente.

c) O *Privacy Impact Assessment* no Reino Unido

Ainda durante a vigência da Diretiva, o Reino Unido, por meio do *Information Commissioner 's Office* (ICO), sua autoridade de proteção de dados, foi o primeiro país do continente europeu a desenvolver, instrumentalizar e publicar uma metodologia de avaliação de riscos ao direito à privacidade.[24] O *Privacy Impact Assessment Handbook* foi publicado em forma de manual em novembro de 2007 e revisto em julho de 2009.[25]

O ICO concentra as competências regulatórias de agência independente, órgão consultivo e administrativo-sancionador para todo o ecossistema britânico de privacidade e proteção de dados pessoais, unificando assim as políticas, ações e interpretações administrativas que tratam do tema, tanto no setor público como no privado. Hoje, a agência cobre a aplicação dos seguintes diplomas legais: *GDPR, Data Protection Act, Freedom of Information Act, Privacy*

[23] "Artigo 28. 2. Os Estados-membros apenas poderão estabelecer a simplificação ou a isenção da notificação nos seguintes casos e condições:
— se, para as categorias de tratamentos que, atendendo aos dados a tratar, não são susceptíveis de prejudicar os direitos e liberdades das pessoas em causa, especificarem as finalidades do tratamento, os dados ou categorias de dados a tratar, a categoria ou categorias de pessoas em causa, os destinatários ou categorias de destinatários a quem serão comunicados os dados e o período de conservação dos dados;
— se o responsável pelo tratamento nomear, nos termos do direito nacional a que está sujeito, um encarregado da proteção dos dados pessoais, responsável nomeadamente por:
— garantir, de modo independente, a aplicação, a nível interno, das disposições nacionais tomadas nos termos da presente diretiva.
— manter um registo dos tratamentos efetuados pelo responsável do tratamento, contendo as informações referidas no nº 2 do artigo 21".
assegurando assim que os tratamentos não são susceptíveis de prejudicar os direitos e liberdades das pessoas em causa". Tradução oficial em português europeu, com singelas modificações. Disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046.

[24] Trilateral Research & Consulting. *Privacy Impact Assesment and Risk Management (2013),* p. 06.

[25] Disponível em:
https://webarchive.nationalarchives.gov.uk/20100402122103/http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/html/0-advice.html.

and Electronic Communications Regulations, Environmental Information Regulations, INSPIRE Regulations, eIDAS Regulation, Re-use of Public Sector Information Regulations, NIS Regulations, Investigatory Powers Act.[26]

Posteriormente à popularização do PIA, o *Cabinet Office*, órgão auxiliar direto do Primeiro-Ministro, reconheceu a eficácia do PIA e estabeleceu a sua obrigatoriedade[27], a partir de julho de 2008, na administração direta e indireta, em caso de novos projetos ou programas que envolvessem quantidades significativas de dados pessoais, como medida mandatória mínima de segurança da informação[28].

Entre as várias definições possíveis para o PIA, adotamos a que seu mentor intelectual principal, Roger Clarke, que comandou a feitura do *Handbook* britânico, entende como a que abarca todos os seus pontos-chave:

> "Privacy impact assessment (PIA) is a systematic process that identifies and evaluates, from the perspectives of all stakeholders, the potential effects on privacy of a project, initiative or proposed system or scheme, and includes a search for ways to avoid or mitigate negative privacy impacts."[29]

Há ainda a definição de David Wright e Paul De Hert[30]:

> "a methodology for assessing the impacts on privacy of a Project, policy, programme, service, product or other initiative which involves the processing of personal information and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts."31

Destas definições, podemos identificar os elementos principais do PIA: ser um *processo* (ou procedimento), não apenas o seu resultado, o relatório; levar em consideração os principais tomadores de decisão (*stakeholders*), ou pessoas atingidas, principalmente, o titular dos dados tratados; identificar e avaliar os efeitos da atividade, sejam positivos ou negativos, co-

[26] As competências regulatórias da agência de fiscalizadora podem ter certa influência, ou até mesmo ser determinante, na amplitude do escopo da avaliação, ora mais amplo, abarcando diversos diplomas legais correlatos, ora mais restrito.
[27] David Tancock, Siani Pearson, Andrew Charlesworth. *The Emergence of Privacy Impact Assessments* (2010). p. 19.
[28] Cabinet Office, Cross Government Actions: *Mandatory Minimum Measures* (2008). Seção I, 4.4.
[29] "A Avaliação de Impacto à Privacidade (PIA) é um processo sistemático que identifica e avalia, a partir da perspectiva de todas as partes interessadas, os efeitos potenciais sobre a privacidade de um projeto, iniciativa, sistema ou esquema proposto, e inclui uma busca por maneiras de evitar ou mitigar impactos negativos sobre a privacidade." tradução livre.
[30] Citado por CABRAL, Filipe F. *O Relatório de Impacto à Proteção de Dados Pessoais como um instrumento para o gerenciamento de riscos na Lei Geral de Proteção a Dados Pessoais – Lei nº 13.709/18.* (2019) Tese (Mestrado em Direito) – Faculdade de Direito. Universidade Estadual do Rio de Janeiro. Rio de Janeiro. p. 88
[31] "Uma metodologia para avaliar os impactos na privacidade de um projeto, política, programa, serviço, produto ou outra iniciativa que envolva o processamento de informações pessoais e, em consulta com as partes interessadas, tomar as ações corretivas necessárias para evitar ou minimizar impactos" – tradução livre.

mo riscos; ser o objeto deste processo de avaliação, ou seja, o direito à privacidade do indivíduo; e determinar esforço do controlador em evitar ou mitigar os impactos negativos no direito à privacidade dos titulares.

Roger Clarke sintetiza os pontos-chave mais importantes do PIA, que os diferenciam de outras atividades da organização: (i) o PIA é realizado em um projeto ou iniciativa específico, o que o diferencia de um programa de compliance geral; (ii) o PIA é antecipatório por natureza, conduzido antes ou durante o desenvolvimento de um projeto, ao invés de em retrospecto (diferente de uma auditoria de proteção de dados e um *compliance check*); (iii) o escopo do PIA é amplo em relação às dimensões da privacidade (*privacy of the person, privacy of personal behaviour and privacy of personal communications*, bem como *privacy of personal data),* possuindo escopo bem mais amplo quando comparado com um DPIA; o PIA tem um escopo amplo em relação às expectativas e perspectivas dos envolvidos que refletem e são incorporadas no projeto, levando em consideração os interesses não só da organização (internos) ou de patrocinadores estratégicos, acionistas, etc., mas também dos segmentos populacionais que serão afetados pelo projeto; (v) o PIA tem amplo escopo no que diz respeito às expectativas com as quais os impactos à privacidade são comparados, incluindo aí as aspirações, necessidades e sentimentos das pessoas e considerações de ordem pública, como o impacto e consequências de um tratamento específico para a sociedade, para a segurança nacional, etc., bem como questões de adequação à(s) lei(s) vigente(s) (o que o diferencia de um *compliance check* ou *assessment (*avaliação de conformidade), seja em adequação às leis de privacidade, em geral, ou a estatutos regulatórios específicos, como leis de proteção de dados (que possuem o foco em privacidade informacional (*data privacy)*; (vi) o PIA é orientado na identificação dos problemas e das soluções, ajustando o projeto, em aplicação do *privacy by design*; (vii) a ferramenta dá ênfase no processo de avaliação, incluindo troca de informações entre setores da organização, *stakeholders* e titulares, aprendizagem organizacional e adaptação do projeto; (viii) o PIA exige engajamento intelectual por parte do alto escalão da organização (CEO's, executivos e gerentes seniores, etc.) e não apenas que ele seja elaborado como mera lista de verificação assinalada por funcionários juniores[32].

[32] CLARKE, Roger. *The Distinction between a PIA and a Data Protection Impact Assessment (DPIA) under the EU GDPR.* For a Panel at CPDP, Brussels, 27 January 2017. Disponível em: http://www.rogerclarke.com/SOS/IA-1401.html, págs. 02-03.

O *Privacy Impact Assessment Handbook* nos traz três ferramentas distintas para a organização implementar. São elas: o *PIA*, a checagem de adequação (*compliance checking*[33]) e a auditoria, cada qual com uma função específica. Inicialmente, o *Handbook* parte para a diferenciação entre elas, levando em conta, principalmente, o grau de maturidade e a implementação do projeto ou sistema, visando sua implementação na rotina da organização, e a factibilidade das recomendações contidas no guia, para que não se tornem penduricalhos burocráticos e ineficazes.

O guia recomenda que *compliance checks* e *data protection audits* sejam utilizados para projetos em fase de implementação ou que já estão em curso há algum tempo, e que o PIA seja utilizado em um estágio em que as recomendações por ele apontadas possam realmente influenciar no desenvolvimento do projeto e serem efetivamente implementadas:

> "The nature of the PIA process means that it is best to complete it at a stage when it can genuinely affect the development of a project. Carrying out a PIA on a project that is up and running runs the risk of raising unrealistic expectations among stakeholders during consultation. For this reason, unless there is a genuine opportunity to alter the design and implementation of a project, the ICO recommends that projects which are already up and running are not submitted to a PIA process, but to either a compliance check or a data protection audit, whichever is more appropriate."[34]

A razão disso é que o esforço da organização e os custos para alterar projetos já em curso são muito maiores que as modificações pontuais na fase de *design* e implementação deles. Além disso, auditorias ou *checklists* de *compliance* pressupõem a existência de leis, regulamentos ou outros instrumentos normativos aos quais o projeto precisa ser adequado. Ou há adequação à lei ou não há. Nesse sentido, o escopo de aplicação do PIA é bem mais amplo que o *compliance check*, porquanto avaliar o impacto de um projeto na perspectiva do direito à privacidade não depende necessariamente das leis vigentes, por ser um aspecto antes social do que juridicamente considerado como elemento normativo.

---

[33] O *compliance checking* e a *data protection audit* não são definidos expressamente pelo Handbook. Estes instrumentos são apenas diferenciados por suas vantagens de acordo com o momento adequado de sua implementação ou deflagração. Todavia, podemos extrair que ambos são instrumentos cuja atividade predominante é a de avaliar um projeto já implementado sob a ótica de sua legalidade ou não, indicando os problemas e propondo eventuais mudanças. Não há menção direta, no guia, dos *compliance risks*, ou os riscos de compliance, que é a avaliação de riscos que a organização realiza.

[34] "A natureza do processo do PIA significa que é melhor concluí-lo em um estágio em que possa afetar genuinamente o desenvolvimento de um projeto. Realizar um PIA em um projeto que está funcionando corre o risco de gerar expectativas irrealistas entre as partes interessadas durante a consulta. Por esse motivo, a menos que haja uma oportunidade genuína de alterar o desenho e a implementação de um projeto, a ICO recomenda que os projetos já em funcionamento não sejam submetidos a um processo de PIA, mas a uma verificação de conformidade ou a dados auditoria de proteção, o que for mais apropriado." – tradução livre. ICO. *Privacy Impact Assessment Handbook* – Version 2.0. p. 03.

O guia recomenda que os *compliance checks* sejam feitos no começo de um projeto, embora só possam ser completados quando o projeto atingir uma forma mais concreta e detalhada[35]. O objeto do *compliance*, por sua vez, não considera apenas um diploma legal, mas todas as normas jurídicas que protejam direta ou indiretamente a privacidade do indivíduo[36]. Todavia, o guia não sugere ou aponta que o *compliance check* seja incompatível ou independente do PIA, permitindo a sua incorporação.

d) O *enfoque* do *Privacy Impact Assessment*: as dimensões da privacidade

O PIA deve considerar o projeto ou tratamento de dados (objeto), contrastando-o com o direito de privacidade do titular, em caráter amplo, com todas as suas dimensões (enfoque de análise), como recomenda o *Handbook*. Para o manual, o direito à privacidade está relacionado à integridade do indivíduo, com diferentes aspectos das suas necessidades sociais. Esses aspectos não são definições estritas que esgotam o debate sobre a problemática.

---

[35] *"Compliance checking should be started at an early stage of the project to address issues such as the legality of any proposed course of action, but this work will normally only be completed later, once the design of the project has reached a more detailed stage." – "A verificação de conformidade deve ser iniciada no estágio inicial do projeto para abordar questões como a legalidade de qualquer curso de ação proposto, mas este trabalho normalmente só será concluído mais tarde, uma vez que o design do projeto tenha alcançado um estágio mais detalhado." (tradução livre). ICO. Privacy Impact Assessment Handbook – Version 2.0. p. 4.*

[36] *"While compliance checking as part of a privacy impact assessment (PIA) will focus on laws which affect privacy, organisations will have to consider broader legal compliance as well. Public sector organisations will have to consider the extent of their powers, any obligations they have in relation to the personal information they collect and any prohibitions on the use of that information. Private sector organisations will have to consider industry standards and law.*
Further documents may be relevant, such as codes of conduct and privacy policy statements, particularly where the organisation has provided some form of undertaking to comply with them. This might arise from membership of an association that issues the code, or the terms of a document that the organisation itself has produced. There are also matters of public policy that may not be formally law, but that are generally respected." – "Embora a verificação de conformidade como parte de uma avaliação de impacto de privacidade (PIA) se concentre nas leis que afetam a privacidade, as organizações também terão que considerar uma conformidade legal mais ampla. As organizações do setor público deverão considerar a extensão de seus poderes, quaisquer obrigações que tenham em relação às informações pessoais que coletam e quaisquer proibições de uso dessas informações. As organizações do setor privado terão que considerar as normas e leis do setor. Outros documentos podem ser relevantes, como códigos de conduta e declarações de política de privacidade, especialmente quando a organização forneceu alguma forma de compromisso para cumpri-los. Isso pode surgir da inscrição em uma associação que emita um código de conduta, ou dos termos de um documento que a própria organização produziu. Existem também questões de ordem pública que podem não ser formalmente lei, mas que são geralmente respeitadas." (tradução livre) Ibidem. p. 47.

O manual nos traz quatro aspectos principais do direito[37]: *the privacy of personal information, the privacy of the person, the privacy of personal behavior and the privacy of personal communications.*[38]

A *privacy of personal information*, também referida como autodeterminação informativa, está relacionada à resistência das pessoas em reconhecer que os dados a ela relacionados estejam expostos/acessíveis facilmente a outros indivíduos e organizações. Daí surge o direito de exercer um controle efetivo sobre o dado e como ele é usado.[39]

---

[37] Ibidem. p.14.

[38] Mantive a nomenclatura dos direitos no original por entender que sua tradução direta pode gerar confusões. Mesmo com o esforço máximo, acredito que esses termos são intraduzíveis pela perda de significado de sua gênese. Esta nomenclatura reflete diretamente a própria concepção do Direito para os britânicos. Traço esse paralelo com o seguinte trecho de Pontes de Miranda, ao falar sobre as diferentes concepções de liberdade, comparando as da *common law* e a dos franceses da Revolução de 1789, cujo raciocínio, *mutatis mutandis*, pode ser aplicado com ressalvas à problemática da privacidade: *"Na Inglaterra, a palavra "liberdade", em direito, sempre vem acompanhada de adjetivo ou de atributo: liberdade pessoal, liberdade de imprensa, etc.*
Todavia a Constituição dos Estados Unidos, conquanto muito extraísse do direito inglês, foi contemporânea da liberdade abstrata, indefinível, e ampla dos pensadores franceses. Eis aí a razão de lá se encontrar, por vezes, aquêle vocábulo desgarrado e sibilino: liberty. Foi sinal dos tempos.
Em que consiste essa liberdade misteriosa, demagógica, nós o sabemos de Montesquieu, no capítulo III do livro XI de seu Espirit des lois: "à pouvoir faire ce que l'on doit vouloir, et à n'être point contraint de faire ce que l'on doit ne point vouloir". Pura liberdade à Robinson Crusoe.
A liberdade inglêsa não é essa. Distinguem-se qualitativamente. Nessa divergência está concretizada a diferença dos caracteres psicológicos dos dois povos. Uma é integral, dogmática, abstrata; a outra é concreta: divide-se, tem espécies… Ora a liberdade de imprensa, ora a liberdade de consciência, ora a liberdade física.
Tôdas concernem a algum objeto sensível. Não são figuras metafísicas. Não volteiam nos domínios da ideologia. Tôdas pisam em terra firme. Não querem o infinito, como aquela: apenas exprimem o conteúdo de seus limites. Se é a liberdade física, define-se em termos verbais invariáveis e salientes: ir, ficar e vir.
Dir-se-à que a outra, a de Paris, é mais bela, mais sedutora. Não há dúvida. Porém mais mentirosa. Promete castelos a quem morre de fome: dá todos os direitos, mas faz depender da opinião exegética do Procurador da Republica a locomoção de alguém. Em vez de ser valor restrito e utilizável, não suscetível de servir a outros intuitos, serve aos maus contra os bons.
Que fêz ela? Nada. Aguilhoou o indivíduo. Criou o mais desbragado capitalismo e deu-o aos menos dignos ("a todos", diz-se; mas os menos dignos tem melhores armas) o direito de explorar homens livres. - Todos são livres; escravizai-vos, agora, uns aos outros!
Sempre foi traço de caráter dos povos inglêses essa precisão a respeito de direitos, coisa em que não os imitaram os escritores franceses. Sirva de exemplo o próprio Parlamento francês. A concepção dilatou-se, fêz-se abstrata, expansiva: em vez de continuar o centro do poder britânico, com as Declarações de direitos, mais escritas nas cabeças do que nos livros e nos discursos.
Onde muito se fala em liberdade, pouco ela é defendida. Corajosamente, até a morte, a sustentam os que, em vez de Liberdade, falam, prática e sabiamente, de liberdade física (de ir, ficar e vir), de liberdade de pensamento, de liberdade de religião (criação de Rhode Island, nos Estados Unidos da América), de liberdade de imprensa, etc." (PONTES DE MIRANDA, História e Prática do Habeas Corpus. 2ª Ed. (1955), José Konfino, pg. 31/32.).

[39] "Individuals generally do not want data about themselves to be automatically available to other individuals and organisations." – "Os indivíduos geralmente não querem que seus dados sejam disponibilizados automaticamente para outros indivíduos e organizações" (tradução livre) ICO. Privacy Impact Assessment Handbook. p.14.

A *privacy of the person* ou *bodily privacy* está relacionada à integridade corporal do sujeito, associada normalmente às revistas corporais, à imunização compulsória, à transfusão de sangue sem consentimento, à entrega compulsória de amostras de tecido ou fluidos corporais, entre outros.

A *privacy of personal behaviour* relaciona-se à noção de *private space*, ou seja, o monitoramento do que um indivíduo faz. Das facetas que a privacidade pode ter na concepção dos britânicos, não sendo uma lista exaustiva, esta é a que mais se assemelha ao clássico conceito de privacidade estadunidense - *the right to be let alone* - desenvolvido até a proteção autônoma e constitucional do *right of privacy.*

A *privacy of personal communications* está atrelada a ideia de proteção da comunicação entre dois indivíduos, seja por qualquer meio, da observância de terceiros não integrantes da relação. No direito brasileiro, entendemos esse aspecto como o sigilo das comunicações pessoais.

Nestes termos, o direito à privacidade, em todas as suas dimensões, não pode ser abarcado por um diploma legal específico. Mesmo considerando a proteção à privacidade em todo o ordenamento jurídico, isso pode não ser suficiente para satisfazer as expectativas das pessoas e as consequências negativas que advêm de uma prática invasiva à privacidade delas.

Mesmo assim, o projeto deve ser avaliado sob o ângulo das leis aplicáveis, no mínimo. Porém, um bom PIA não deve se limitar às leis vigentes e aplicáveis ao projeto. As necessidades, expectativas e preocupações dos indivíduos, grupos de indivíduos e comunidades, muitas vezes, não estão refletidas diretamente na legislação vigente. Não é incomum encontrar casos de projetos e sistemas que, embora estejam de acordo com as leis aplicáveis, por não se preocuparem de fato, sofrem uma cobertura negativa da mídia, e por reflexo da opinião pública, o que pode minar sua confiança e acabar com a sua descontinuidade.[40]

e) O *Data Protection Impact Assessment* no *GDPR* e o controle prévio

[40] "Organisations that carry out a DPIA may be fully compliant with data protection legislation, but could still intrude dangerously into an individual's privacy. Such a risk is greatly diminished if all types of privacy are considered, as the ICO Handbook rightly argues.". "Organizações que realizam uma DPIA podem estar em total conformidade com a legislação de proteção de dados, mas ainda podem invadir perigosamente a privacidade de um indivíduo. Esse risco diminui muito se todos os tipos de privacidade forem considerados, como o Manual da ICO corretamente argumenta" (tradução livre). *Privacy impact assessment and risk management* (2013). Report for the Information Commissioner's Office prepared by Trilateral Research & Consulting, p. 149.

Como dito, o sistema de notificação geral e checagem prévia da Diretiva foi substituído, optando-se por outras alternativas mais eficazes à proteção de dados pessoais dos indivíduos, exposta no considerado (ou *recital)* 89 do *GDPR*:

> "Além de esta obrigação originar encargos administrativos e financeiros, nem sempre contribuiu para a melhoria da proteção dos dados pessoais. Tais obrigações gerais e indiscriminadas de notificação deverão, por isso, ser suprimidas e substituídas por regras e procedimentos eficazes mais centrados nos tipos de operações de tratamento suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, devido à sua natureza, âmbito, contexto e finalidades. Os referidos tipos de operações de tratamento poderão, nomeadamente, envolver a utilização de novas tecnologias, ou pertencer a um novo tipo e não ter sido antecedidas por uma avaliação de impacto sobre a proteção de dados por parte do responsável pelo tratamento, ou ser consideradas necessárias à luz do período decorrido desde o tratamento inicial responsável pelo tratamento."[41]

A consulta prévia (*prior consultation*) consiste em notificar a autoridade nacional respectiva apenas quando há "altos riscos" residuais ao tratamento de dados, isto é, após todas as medidas de mitigação identificadas pelo controlador forem implementadas.

Há duas diferenças na sistemática da Diretiva e do atual *GDPR*: (i) os gatilhos que exigem atuação da autoridade nacional são diferentes. Na primeira, realizava-se a checagem prévia, quando identificados altos riscos iniciais no tratamento, (o risco bruto), e na segunda, somente quando há altos riscos residuais; e (ii) no GDPR, a ausência de resposta da autoridade nacional, quando provocada, não implica em autorização da atividade.[42]

Percebe-se, nesta mudança, que há o constante esforço de afunilamento e aperfeiçoamento para que a atuação das autoridades nacionais se dirija quando ela for *realmente necessária*, concentrando os esforços justamente nas situações mais críticas.

O DPIA deverá prosseguir, de forma que todos os riscos aos direitos e liberdades individuais sejam identificados e avaliados. As medidas de mitigação a esses riscos e salvaguardas deverão ser implementadas, e depois de sua implementação pelo controlador, caso estas se mostrem insuficientes e ainda restem riscos residuais altos que não podem ser mitigados, ou em caso de dúvida na mitigação, o controlador deverá proceder com a consulta prévia à autoridade nacional do respectivo estado membro, para que esta analise o DPIA enviado e forneça o auxílio consultivo necessário.

---

[41] GDPR. Considerando 89.

[42] EDPS. *Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation* (2019). p. 21.

Há uma relação entre o registro de atividades de processamento (ROPA)[43], entre os DPIA's e a consulta prévia. O registro é para todas as operações; o DPIA é para operações que apresentam altos riscos aos direitos e liberdades fundamentais do titular; e a consulta prévia, para quando há altos riscos residuais[44]. O *GDPR* estabeleceu como ferramenta típica para avaliação dos altos riscos e sua mitigação o DPIA.

O desenvolvimento e a experiência do Reino Unido popularizaram o uso dos PIA's pela Europa, o que culminou no *Data Protection Impact Assessment* (DPIA). A definição do que é a ferramenta se encontra no artigo 35, 1.:

> "Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação."[45]

O *DPIA* é um processo de avaliação que é deflagrado em um momento bem específico: quando, antes de se iniciar uma atividade de tratamento, identificam-se altos riscos aos direitos e liberdades fundamentais do titular.

A realização do relatório pode ser dispensada quando se verificar que: (i) o tratamento não enseje altos riscos; (ii) quando a natureza, o âmbito, o contexto e as finalidades do tratamento forem muito semelhantes ao tratamento em relação ao qual tenha sido realizada um DPIA; (iii) quando as operações de tratamento tiverem sido previamente controladas por uma autoridade de controle do GDPR em condições específicas que não se tenham alterado; e (iv) quando uma operação de tratamento for fundada como necessária para o cumprimento de obrigação legal ou regulatória pelo controlador ou necessária para atender ao interesse público (nos termos do artigo 6º, nº 1, alíneas c) ou e) do GDPR e que tal avaliação já tenha sido realizada como parte da adoção desse fundamento jurídico (GDPR, artigo 35.º, n.º 10), salvo se o Estado-Membro considerar necessário proceder a essa avaliação antes das atividades de tra-

[43] GDPR, Artigo 31.
[44] EDPS. *Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation*. (2019). p. 20.
[45] GDPR. Art. 35.1, versão em português europeu.

tamento; ou (v) quando o tratamento for listado pela Autoridade Nacional respectiva como opcional ao DPIA. [46]

Portanto, além de um esforço para concentrar a atuação da autoridade nacional de proteção de dados, há um esforço em manter a máxima clareza de quando o DPIA deve ser deflagrado[47], e, ainda, não onerar desnecessariamente os agentes de tratamento, possibilitando o aproveitamento de avaliações semelhantes, sejam feitas por si ou por outrem, com as respectivas medidas de mitigação.

O relatório deverá ser acompanhado e assinado pelo *data protection officer (DPO),* equivalente ao encarregado da LGPD, nos casos em que for designado. No *GDPR*, é obrigatório designá-lo: (i) caso o controlador seja uma autoridade ou órgão público (exceto para o Judiciário atuando em sua competência jurisdicional); (ii) caso as atividades de tratamento realizem monitoramento regular e sistemático em larga escala dos indivíduos; ou (iii) caso as atividades principais de tratamento de dados do controlador consistam em processamento em larga escala de dados sensíveis ou de dados relacionados a condenações e delitos criminais.

Todavia, a escolha e adoção dessa ferramenta não é imune às críticas, tais como: (i) a de ser um fardo desnecessário, uma burocracia desproporcional, o que causa aumento de despesa e atrasa a tomada de decisão por parte dos agentes de tratamento, e por consequência o desenvolvimento do projeto; (ii) a complexidade do processo de avaliação na prática, as dificuldades que acarreta, a ausência de experiência da organização, bem como ausência de orientação por parte das autoridades competentes; (iii) a incerteza do valor do DPIA em relação a outras técnicas de avaliação (como *compliance checks* ou auditorias), bem como sua eficácia para os direitos dos titulares, considerando a ampla discricionariedade concedida sobre "como" e "se" tais avaliações devem ser conduzidas ou não; (iv) quando o DPIA é exigido por lei em certa hipótese, representa apenas instrumento de *compliance* regulatório, de escopo restrito, o que faz projetos e iniciativas consideravelmente invasivos, perigosos ou danosos serem

46 WP29. *Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679* – p. 15.

47 O rol exemplificativo de operações que ensejam em alto risco do GDPR é complementado com um guia de critérios da WP29 sobre operações de tratamento a que o controlador deve ficar atento. Além disso, há as *blacklists* emitidas pelas autoridades nacionais, que são inspiradas nos critérios da WP29 e complementam as hipóteses de alto risco do rol legal. Outro ponto que demonstra isso é o histórico dos pareceres da EDPB sobre as *blacklists* de cada autoridade nacional, zelando pela integridade e semelhança do *GDPR* no bloco, e portanto, da clareza dos critérios.

desconsiderados; v) a falta de transparência, tendo em vista a complexidade da análise ou do projeto em si mesmo considerado, e, por conseguinte, de resultados finais e recomendações, o que torna a avaliação opaca ao escrutínio público e aos afetados pela iniciativa; vi) além da opacidade, a consulta pública e dos afetados pelo tratamento, por estarem sujeitos ao juízo de discricionariedade do controlador dos dados, tornam-se mero "faz de conta".[48]

Roger Clarke tece diversas críticas sobre o DPIA, em ocasião do então recém aprovado artigo 35.1 do GDPR: (i) o DPIA não é movido por valores sociais; (ii) será interpretado apenas como uma *Data Protection Law Compliance Assessment (*i.e. uma avaliação de *compliance* com certa lei de proteção de dados); (iii) possui escopo de proteção reduzido quando comparado com avaliações de impacto à privacidade informacional (*data privacy*), e menos ainda quando comparado com o PIA, que encampa todas as dimensões da privacidade. (iv) quanto ao escopo de atuação, aplica-se apenas ao subconjunto de interesses (ou pretensões) relativas à privacidade informacional do titular regulados por uma lei de proteção de dados vigente, escopo de proteção bem reduzido se o objeto de adequação da avaliação fosse o impacto à privacidade informacional, ou mesmo em caso de adequação a todas as leis/regulamentações vigentes acerca de privacidade informacional;[49]

Além disso, Clarke aponta que as organizações já estão sujeitas à obrigação de se adequar a lei em caso de implementação de novas iniciativas e projetos, o que o torna desnecessário, e que as inovações do art. 35 do GDPR em nada avançam em proteção à privacidade, citando um leve progresso em relação às obrigações de descrição sistemática do tratamento e da avaliação da necessidade e proporcionalidade do tratamento (GDPR, Art. 35, 7.). Para elucidar tais críticas, Clarke propõe uma situação hipotética, de modo a convidar o leitor à reflexão:

> "CCTV, body-worn cameras and drone-borne cameras may record data. But they can also stream data to an observer without recording it. And they can also cause people concern just by being there without being switched on - and indeed the mere possibility that they may be around is upsetting to various individuals under various circumstances.
> Where visual surveillance doesn't give rise to any recorded data:
> (a) can a DPIA consider the impact on the privacy of personal behaiour of:

[48] Kloza, Dariusz & Dijk, Niels & Gellert, Raphaël & Böröcz, István & Tanas, Alessia & Mantovani, Eugenio & Quinn, Paul. (2017*). Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals*. p. 03.

[49] CLARKE, Roger. *The Distinction between a PIA and a Data Protection Impact Assessment (DPIA) under the EU GDPR.* For a Panel at CPDP, Brussels, 27 January 2017. Disponível em: http://www.rogerclarke.com/SOS/IA-1401.html. p. 03.

(i) the operation of cameras?
(ii) the existence of cameras?
(iii) the possibility of the existence of cameras?
(b) *must* a DPIA ... (etc.)?"[50]

f) O elemento alto risco

i. Riscos de compliance e riscos ao titular

Como se viu anteriormente, tanto no PIA quanto no DPIA, a ferramenta torna-se obrigatória a partir da identificação do elemento "riscos específicos" ou "altos riscos" – que podem ser entendidos como sinônimos. A obrigatoriedade de elaboração do DPIA é extraída: (i) das listas de operações de alto risco emitidas pela autoridade nacional competente; ou (ii) da avaliação inicial de riscos do tratamento, feita pelo próprio controlador.[51] Em ambas as ocorrências, pode-se ver que a presença do elemento "alto risco" é imprescindível para que a ferramenta se torne obrigatória.

Inicialmente, cabe ressaltar que os riscos em proteção de dados possuem ângulos distintos de análise. Pode-se analisá-los do ponto de vista da organização e do ponto de vista do titular. Os primeiros são os riscos de *compliance*, ou seja, os riscos que a organização corre em não se adequar à legislação, que também podem abarcar danos na sua imagem, em descontentamento social, etc. Os segundos são os riscos aos direitos e às liberdades fundamentais do titular. No DPIA, os riscos devem ser avaliados primariamente do ponto de vista do titular de dados, mas nada impede que o mesmo relatório contenha uma avaliação de riscos de *compliance.*[52]

---

[50] Ibidem. CFTV (circuito fechado de televisão), câmeras corporais e câmeras portadas por drones podem registrar dados. Mas eles também podem transmitir dados para um observador sem gravá-los. E também podem causar preocupação às pessoas apenas por estarem presentes sem estarem ligados - e, de fato, a mera possibilidade de que possam estar por perto é perturbadora para vários indivíduos em várias circunstâncias.
Onde a vigilância visual não dá origem a nenhum dado registrado:
(a) um DPIA pode considerar o impacto sobre a privacidade do comportamento pessoal:
(i) do funcionamento das câmeras?
(ii) da existência de câmeras?
(iii) da possibilidade da existência de câmeras?
(b) * deve * um DPIA fazê-lo?... (etc.)?" (tradução livre).

[51] EDPS. *Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments (*2018). p. 09.

[52] "*In a DPIA, you assess primarily risks to the rights and freedoms of data subjects. At the same time, you should analyse the compliance risks for your organisation. These are related, but not necessarily identical."* – " Em um DPIA, você avalia principalmente os riscos aos direitos e liberdades dos titulares dos dados. Ao mesmo tempo, você deve analisar os riscos de conformidade para sua organização. Eles estão relacionados, mas não necessariamente idênticos." (tradução livre). EDPS. *Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation* (2019)**.** p. 08.

Pode-se encontrar uma elucidação de como o risco pode ser materializado para o titular no Considerando 75, do GDPR:

> "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."[53]

É importante considerar, no DPIA, todo e qualquer risco que possa prejudicar, direta ou indiretamente, a autonomia individual da pessoa em causa, e isso leva em consideração impactos emocionais como o medo, a angústia, a supressão, ou o efeito inibidor que certo tratamento pode gerar nos direitos e nas liberdades fundamentais, como, por exemplo, vigilância, controle e rastreamento contínuo, afetando potencialmente as liberdades de ir e vir, de intimidade, e de liberdade de expressão, além de, principalmente, os aspectos de probabilidade do evento danoso e da severidade do dano.

Outro ponto importante é que o "impacto" avaliado não deve ser somente considerado no eixo da quantidade. Não se pode avaliar o risco unicamente na quantidade de pessoas afetadas pelo processamento. Sem dúvida, este é um fator importante, mas o principal a ser considerado é o eixo qualitativo, que é justamente o impacto nos direitos e nas liberdades não só do titular individualmente considerado, mas da sociedade como um todo.

A avaliação de riscos inerentes ao tratamento não deve se resumir a precauções contra incidentes de segurança. Projetos que envolvam o uso de novas tecnologias, por exemplo, podem causar um dano muito mais acentuado se realizado de uma maneira imprudente, como

[53] Versão em português europeu.

um tratamento discriminatório ilícito, causado por dados enviesados e utilizados para o treinamento do aprendizado de máquina.

A análise do elemento risco, portanto, não está limitada a riscos de *compliance*, de descumprimento da lei, a riscos que atentem contra a dimensão da *data privacy*, do indivíduo, a riscos que atentem contra sua privacidade, considerando todas as dimensões envolvidas. Os riscos devem ser avaliados levando-se em conta os direitos e as liberdades fundamentais. Neste ponto, não há como traçar uma régua limite, e tudo que puder afetar negativamente o titular deve ser considerado para que seja mitigado posteriormente.

ii. A obrigatoriedade do DPIA

O GDPR exigiu a elaboração do relatório, estabelecendo que certos tipos de tratamento, por sua natureza, âmbito, contexto e finalidade, podem implicar em um elevado risco para os direitos e as liberdades das pessoas, e nestes casos o controlador deverá, antes de iniciar o tratamento, proceder com um DPIA[54].

O Regulamento exemplificou algumas operações típicas de ensejar num alto risco, e por conseguinte, sua obrigatoriedade: (a) avaliação sistemática e completa dos aspectos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar; (b) operações de tratamento em grande escala de dados pessoais sensíveis ou equiparados ou relacionados com condenações penais, infrações, medidas de segurança e afins; e (c) controle sistemático de zonas acessíveis ao público em grande escala.[55]

O relatório deve conter, no mínimo: "a) Uma descrição sistemática das operações de tratamento previstas e a finalidade do tratamento, inclusive, se for caso disso, os interesses legítimos do responsável pelo tratamento; (b) Uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos; c) Uma avaliação dos riscos para os direitos e liberdades dos titulares dos direitos a que se refere o nº 1; e (d) As medidas previstas para fazer face aos riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com

[54] GDPR, Art. 35, item 1.
[55] GDPR, Artigo 35, versão em português europeu.

o presente regulamento, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa"[56].

Ainda, o Regulamento estabelece competência para cada Autoridade de Nacional de Proteção de Dados de cada Estado Membro estabelecer, baseados nos critérios elaborados pelo *Working Party 29*, expostos a seguir, uma lista de operações de "alto risco", tendo como consequência a necessidade de consulta prévia à autoridade para iniciar o tratamento. Essa formulação legal teve como base os estudos realizados pelo WP29, hoje substituído pelo Comitê Europeu para a Proteção de Dados (EDPB), intitulado *"Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679"*.

O WP29 estabeleceu nove critérios em que a operação de tratamento enseja num alto risco, e pontuou que, na maioria dos casos, se a atividade de tratamento "cair" em pelo menos dois critérios, a feitura do DPIA é recomendada. Os critérios são:

> "1. Avaliação ou classificação, incluindo definição de perfis e previsão, em especial de «aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados» (considerandos 71 e 91 da GDPR).
> 2. Decisões automatizadas que produzam efeitos jurídicos ou afetem significativamente de modo similar: tratamento destinado à tomada de decisões sobre os titulares dos dados e que produza «efeitos jurídicos relativamente à pessoa singular» ou que «a afetem significativamente de forma similar» (artigo 35.º, n.º 3, alínea (a).
> 3. Controle sistemático: tratamento utilizado para observar, monitorizar ou controlar os titulares dos dados, incluindo dados recolhidos através de redes, ou um «controlo sistemático de zonas acessíveis ao público» (artigo 35.º, n.º 3, alínea (c).
> 4. Dados sensíveis ou dados de natureza altamente pessoal: inclui categorias especiais de dados pessoais, tal como definido no artigo 9.º (por exemplo, informações acerca das opiniões políticas dos indivíduos), bem como dados pessoais relacionados com condenações penais e infrações, tal como definido no artigo 10.º.
> 5. Dados tratados em grande escala: o RGPD não define o que constitui grande escala, contudo o considerando 91 fornece alguma orientação. Em qualquer caso, o Grupo de Trabalho do Artigo 29.º recomenda que os seguintes fatores, em especial, sejam considerados quando se determina se o tratamento é ou não efetuado em grande escala:
> a. o número de titulares de dados envolvidos, quer através de um número específico quer através de uma percentagem da população pertinente;
> b. o volume de dados e/ou a diversidade de dados diferentes a tratar;
> c. a duração da atividade de tratamento de dados ou a sua pertinência;
> d. a dimensão geográfica da atividade de tratamento.
> 6. Estabelecer correspondências ou combinar conjuntos de dados: por exemplo, com origem em duas ou mais operações de tratamento de dados realizadas com diferentes finalidades e/ou por diferentes responsáveis pelo tratamento de dados de tal forma que excedam as expectativas razoáveis do titular dos dados.

[56] GDPR, artigo 35, nº 7. versão em português europeu.

> 7. Dados relativos a titulares de dados vulneráveis (considerando 75): o tratamento deste tipo de dados constitui um critério devido ao acentuado desequilíbrio de poder entre os titulares dos dados e o responsável pelo tratamento dos dados, significando isto que os indivíduos podem não ser capazes de consentir, ou opor-se, facilmente ao tratamento dos seus dados ou de exercer os seus direitos. Os titulares de dados vulneráveis podem incluir crianças, empregados, segmentos mais vulneráveis da população que necessitem de proteção especial (pessoas com doenças mentais, requerentes de asilo, idosos, doentes, etc.) e todos os casos em que possa ser identificado um desequilíbrio na relação entre a posição do titular dos dados e o responsável pelo tratamento.
> 8. Utilização de soluções inovadoras ou aplicação de novas soluções tecnológicas ou organizacionais, tais como combinar a utilização da impressão digital e do reconhecimento facial para melhorar o controlo do acesso físico, etc. O RGPD deixa claro (artigo 35.º, n.º 1, e considerandos 89 e 91) que a utilização de uma nova tecnologia, definida em «conformidade com o nível de conhecimentos tecnológicos alcançado» (considerando 91), pode desencadear a necessidade de realização de uma AIPD. As consequências pessoais e sociais da implantação de uma nova tecnologia podem ser desconhecidas. Uma AIPD ajudará o responsável pelo tratamento de dados a compreender e dar resposta a esses riscos. Por exemplo, algumas aplicações da «Internet das Coisas» podem ter um impacto significativo na vida quotidiana e na privacidade dos indivíduos e, como tal, exigem a realização de uma AIPD.
> 9. Quando o próprio tratamento impede os titulares dos dados «de exercer um direito ou de utilizar um serviço ou um contrato» (artigo 22.º e considerando 91). Estão incluídas operações de tratamento destinadas a autorizar, alterar ou recusar o acesso dos titulares dos dados a um serviço ou que estes celebrem um contrato."[57]

g) O RIPD e o pia na lei geral de proteção de dados pessoais

i. A Avaliação de Impacto à Privacidade

Inicialmente, é possível extrair do texto da LGPD a presença tanto de uma avaliação de impacto à privacidade, especificamente no art. 50, §2º, inciso I, alínea (d)[58], como de um relatório de impacto à proteção de dados pessoais (RIPD), em capítulos e momentos distintos. A avaliação de impacto à privacidade, como regulamentada na LGPD, é substancialmente diferente do RIPD. A primeira ferramenta é medida de boas práticas, enquanto a segunda é

[57] WP29. *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (2017)*. Versão em português europeu. p. 10-12.

[58]: "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.
§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:
I - implementar programa de governança em privacidade que, no mínimo:
d) estabeleça políticas e salvaguardas adequadas *com base em processo de avaliação sistemática de impactos e riscos à privacidade"*.

obrigatória assim que preenchidas certas condições, de modo que não elaborar um RIPD, quando necessário, pode ensejar em sanções.

Essa avaliação sistemática de impacto à privacidade representa uma semelhança maior com o *Privacy Impact Assessment*, que possui *enfoque* de avaliação bem mais amplo do que o RIPD, que, seguindo os passos do *GDPR,* é uma ferramenta para demonstrar *compliance*. Por estas razões, discordamos da afirmação de Maria Gomes sobre a menção à avaliação sistemática de impactos e riscos à privacidade na lei:

> "se apresenta como uma fase predecessora da elaboração do relatório, uma vez que é necessário primeiro verificar, através de uma avaliação, conduzida e estruturada mediante uma metodologia, sendo, neste caso, uma metodologia avaliativa de riscos, o impacto de operações de tratamento em liberdades civis e direitos fundamentais do ser humano, aqui compreendido como titular dos dados[59].

A lei brasileira, ainda, estabelece a obrigação do controlador em realizar e documentar avaliações de risco, notadamente em três hipóteses: (i) na elaboração e documentação do Relatório de Impacto à Proteção de Dados Pessoais (RIPD); (ii) para saber se comunicará ou não a ANPD acerca do incidente de segurança[60]; e (iii) na avaliação se o tratamento está em desacordo com a legislação, avaliando *"o resultado e os riscos que razoavelmente dele se esperam"*[61]. Desse modo, a LGPD segue a mesma abordagem do GDPR: uma abordagem regulatória baseada em direitos fundamentais com situações específicas de análise de risco.

ii. O Relatório de Impacto à Proteção de Dados

Quanto ao RIPD, a sua importação em um cenário como o brasileiro e a ótica que lhe tem sido dada revelaram-se problemáticas e desafiadores por diversos fatores. Em seu glossário, a LGPD traz o relatório como *"documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco"*[62]. O relatório *"deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a aná-*

[59] GOMES, Maria Cecília Oliveira. *Relatório de Impacto a Proteção de Dados Pessoais: uma breve análise da sua definição e papel na LGPD* (2019), Revista da AASP, n. 144. p. 07.
[60] LGPD, Art. 48. *"O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.*". À semelhança do GDPR, este artigo traz a possibilidade de que a ANPD considere a desnecessidade de comunicação de incidentes de segurança que entender como irrelevantes aos titulares, o que implica uma avaliação do risco, mesmo que simplificada.
[61] LGPD, Art. 44, inciso II.
[62] LGPD, Art. 5º, inciso XVII.

lise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados."[63]

Na definição dada pela LGPD e no conteúdo mínimo do relatório, analisando apenas a letra fria da lei, podemos perceber que ele se distancia bastante da definição dada pelo GDPR, com os conceitos-chaves de processo, de "alto risco", da avaliação de necessidade do tratamento, entre outros, inicialmente ignorados. A única menção ao "alto risco", o que é elemento central do PIA e do DPIA, se encontra no Art. 55-J, inciso XIII da lei:

> "Art. 55-J. Compete à ANPD:
> XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei".

Na verdade, o "relatório de impacto" como insculpido na lei[64] assemelha-se muito mais à junção do *Record of Processing Activities* (ROPA) com uma espécie de *risk assessment.*

Traçando um paralelo com o cenário europeu, no qual o DPIA sofreu diversas críticas, no Brasil, destacam-se alguns agravantes: a abordagem excessivamente formalista que é possível extrair do texto da lei; uma possível amplitude das suas hipóteses de elaboração sem uma proporcionalidade aparente, despregada das reais funções da ferramenta e a ausência de critérios claros para quando elaborá-lo, o que não passou incólume a críticas. Matheus Sturari, a título de exemplo, explorou tais pontos problemáticos extraídos da lei:

> "Constata-se, por dedução da definição do art. 5º, XVII, que o DPIA será exigido para atividades de tratamento que gerem *riscos às liberdades civis e direitos fundamentais.* Entretanto, são várias as dúvidas que permanecem, por exemplo: (i) toda hipótese de tratamento fundamentado em legítimo interesse deve ser acompanhada de um DPIA?; (ii) quais são os tratamentos que serão considerados como geradores

[63] LGPD, art. 38, parágrafo único.

[64] Na LGPD, no texto da lei somente há obrigação expressa do controlador em manter o registro de atividades de tratamento, sem maiores detalhes, o que está previsto art. 37, caput: *"O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse."* Logo em seguida, há uma previsão legal do poder da ANPD em requisitar a elaboração do relatório: *"Art. 38: A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial"*. Estes dois elementos dão a entender que o registro das operações de tratamento e o relatório de impacto são ferramentas autônomas e independentes, em contraposição com a interpretação literal da definição legal do RIPD (inciso XVII do art. 5º) e de seu conteúdo (parágrafo único do art. 38).

> de riscos a ponto de demandarem um DPIA?; (iii) a despeito de uma lista, quais critérios devem ser considerados para analisar a existência de risco e considerar a necessidade de um DPIA?; (iv) todo e qualquer risco deve ensejar um DPIA ou apenas "alto" risco, como no inciso XIII do art. 55-J?"[65]

Destaca-se, também, a sua crítica:

> "Tais dúvidas parecem surgir em razão de uma preocupação da LGPD sob aspecto formal relacionado ao DPIA, isto é, estabelecendo o que deveria ser considerado em seu instrumento (relatório), mas ausência de tratativa, pela lei, referente ao seu aspecto processual, ou seja, não como um mero documento, mas como um processo de análise que deve ser desencadeado de acordo com critérios claros e, preferencialmente, dotados de certo aspecto objetivo. A LGPD parece focar no resultado de DPIA -- o relatório --, mas pareceu silenciar acerca de todo o processo necessário para se chegar a tal relatório, inclusive o principal -- quando tal processo deve ser desencadeado. Acontece que, a existência de tais dúvidas e de um cenário de incertezas envolvendo o tema, tem gerado um efeito que, a meu ver, pode não ser positivo: a possível banalização do DPIA e consequente excessiva oneração dos agentes de tratamento." (grifos do autor).[66]

Estes fatores não indicam uma interpretação nacional, adaptada ao cenário regulatório brasileiro de proteção de dados, mas uma possível "banalização" da ferramenta, na expressão de Matheus Sturari. Nesse mesmo sentido, segue a crítica de Filipe Fonteles Cabral:

> "há o risco de que o RIPD se torne um instrumento de controle em casos isolados ou, pior, que seja um documento elaborado para fins formais, porém sem guiar uma atividade real de gerenciamento de riscos, o que pode comprometer a eficácia do sistema de proteção aos dados pessoais no Brasil."[67]

Os autores nacionais tendem a ressaltar o caráter procedimental, de *documento-vivo,* do relatório, justamente para reverter as incongruências da lei, que resultaria na ineficácia do relatório e do sistema de proteção de dados como um todo.

Todavia, o problema não termina aí. Na evolução das ferramentas, houve um constante esforço para otimizar a atuação das autoridades de proteção de dados nos casos *realmente necessários* e para não onerar excessivamente o controlador de dados com o processo complexo de análise que é uma avaliação de impacto.

---

[65] STURARI, Matheus. *O DPIA na LGPD: interpretação nacional ou banalização do instrumento***?** Perfil do LinkedIn. Publicado em 29 de outubro de 2020. Disponível em: https://www.linkedin.com/pulse/o-dpia-na-lgpd-interpreta%C3%A7%C3%A3o-nacional-ou-banaliza%C3%A7%C3%A3o-do-matheus/.

[66] Ibidem.

[67] CABRAL, Filipe F. *O Relatório de Impacto à Proteção de Dados Pessoais como um instrumento para o gerenciamento de riscos na Lei Geral de Proteção a Dados Pessoais – Lei nº 13.709/18. (*2019) Tese (Mestrado em Direito) – Faculdade de Direito. Universidade Estadual do Rio de Janeiro. Rio de Janeiro. p. 82.

Ocorre que, a mera possibilidade de o relatório ser requisitado[68] diretamente por uma autoridade, para além do critério de alto risco, vai na contramão do controle prévio do *GDPR*, e até mesmo da checagem prévia da Diretiva.

A presença do encarregado de dados e as suas garantias de independência existem justamente para que este realize a comunicação com a ANPD, e não o inverso. Além disso, um eventual cenário de frequente requisição direta de elaboração do relatório pela ANPD demonstra dois sintomas: o primeiro, os critérios para a sua obrigatoriedade não são claros o suficiente, o que pode ser corrigido via ato normativo da autoridade; o segundo, o fracasso completo do RIPD como ferramenta *ex ante,* visto que se os critérios para a sua obrigatoriedade são obscuros, tampouco impedem a implementação de processamento, prossegue-se com a atividade de alto risco, para elaborar o relatório apenas quando solicitado diretamente. Em suma, uma verdadeira carta-branca para o não cumprimento da obrigação de *compliance*.

A Autoridade Nacional teria que, às cegas, identificar os controladores cujas atividades atraiam a necessidade de *enforcement*, requisitar a elaboração do relatório, dar um prazo específico, receber o relatório, avaliar se ele foi elaborado corretamente, se há altos riscos iniciais, e se há altos riscos residuais, para então conseguir auxiliar o controlador e verificar a conformidade.

Esse tipo de abordagem dissipará o tempo e esforço da recém-criada ANPD para onde ela é realmente necessária. O momento mais adequado para a identificação, pela ANPD, se o controlador cumpriu com as suas obrigações de elaborar o RIPD (avaliar conformidade, identificar riscos e mitigá-los) é em uma notificação de vazamento de dados.

Além de estar sujeito a pura discricionariedade, ou na melhor das hipóteses, de uma discricionariedade vinculada, a requisição pode onerar os controladores que não possuem atividades de alto risco, apenas porque uma autoridade requisitou o relatório, que será feito às pressas, apenas para ser entregue, desprovido de todas as suas funções principais.

4 CONCLUSÕES

O processo de elaboração do PIA/DPIA possui várias etapas que podem variar de acordo com a metodologia adotada ou com as recomendações da autoridade nacional respectiva. Entretanto, podemos dividi-lo em quatro eixos principais: (i) *o eixo da análise de sua*

[68] Seja a sua elaboração ou mera requisição de envio à autoridade.

necessidade; (ii) o eixo da avaliação de adequação (*compliance*), que é uma avaliação predominantemente jurídica; (iii) o eixo da avaliação de impactos e riscos; e (iv) o eixo da implementação de medidas adequadas e proporcionais para a mitigação dos impactos e riscos identificados.

No primeiro eixo, a obrigatoriedade legal do relatório nasce de tratamentos de dados que gerem altos riscos aos direitos e às liberdades fundamentais. A necessidade pode ser extraída de tratamentos de dados presumidos por lei ou regulamento a ensejar alto risco, ou em uma análise interna feita pelo controlador.

No segundo eixo, o *objeto* (projeto, sistema, tratamento, etc) da avaliação deve *enfoque* mínimo limitado. No cenário brasileiro, o *enfoque* de adequação mínimo dado ao RIPD pode ser a LGPD, somente, ou a LGPD em conjunto com outros diplomas legais que incidam sobre a atividade de tratamento (e.g. LGPD + ECA, LGPD + CDC, etc.), para que o controlador saiba se cumpriu adequadamente a sua tarefa e prossiga com a próxima etapa. Se a atividade de tratamento não possui os padrões mínimos de adequação à lei, mesmo que se avalie e mitigue os riscos, isso não sanará os vícios originários da atividade, e, portanto, descumprirá a lei diretamente. Por exemplo, não faz sentido que se proceda uma avaliação de impacto ambiental após a instalação e o funcionamento de uma fábrica, para depois adequá-la para mitigar os riscos identificados. Também não faz sentido que se proceda com uma avaliação de riscos à segurança do trabalho em determinada empreitada após a construção do edifício.

No terceiro eixo, não há limitação de *enfoque* para a avaliação dos riscos. Não se pode limitar os riscos, do ponto de vista do titular, aos riscos de proteção de dados. Tudo que puder influenciar, positiva ou negativamente, os direitos e as liberdades, deve ser levado em conta.

No quarto eixo, os riscos identificados devem ser mitigados por medidas de segurança, técnicas ou administrativas *adicionais,* suficientes para sua mitigação até um nível aceitável. Neste eixo, pode haver o controle prévio da autoridade ou não, a depender da legislação aplicável. Como vimos, no *GDPR* há esse controle quando há altos riscos residuais.

Para não relegar o RIPD à sua banalização, a ferramenta deve ser entendida como uma abordagem *escalável e proporcional* ao *compliance,* em que a identificação do elemento "alto risco", antes mesmo se proceder com detalhes sobre o projeto, e muito antes de iniciar sua implementação, para a deflagração de sua obrigatoriedade, são seus elementos centrais e in-

dissociáveis, assim como no *GDPR*, de forma a focar os esforços da ANPD para as situações críticas, antes que o dano ocorra, e também para não onerar desnecessariamente o controlador.

BIBLIOGRAFIA

Cabinet Office, Cross Government Actions: **Mandatory Minimum Measures**. 2008.

CABRAL, Filipe F. **O Relatório de Impacto à Proteção de Dados Pessoais como um instrumento para o gerenciamento de riscos na Lei Geral de Proteção a Dados Pessoais. Lei nº 13.709/18.**

CLARKE, Roger. An evaluation of privacy impact Assessment guidance documents (2011). **International Data Privacy Law**, Vol. 1, No. 2, 2011.

CLARKE, Roger. Approaches to Impact Assessment. Exhibit 1: Assessment Categories. According to Focus. **Rogerclarke**, 2014. Disponível em: http://www.rogerclarke.com/SOS/IA-1401.html#AF.

CLARKE, Roger. Privacy Impact Assessment: Its Origins and Development, Roger Clarke, **Computer Law & Security Review,** 25, 2, 2009.

CLARKE, Roger. The Distinction between a PIA and a Data Protection Impact Assessment (DPIA) under the EU GDPR. For a Panel at CPDP, Brussels. **Rogerclarke**, 27 January 2017. Disponível em: http://www.rogerclarke.com/SOS/IA-1401.html.

DIRETIVA 95/46/EC.

EDPS. **Accountability on the ground Part I:** Records, Registers and when to do Data Protection Impact Assessments. 2018.

EDPS. **Accountability on the ground Part II:** Data Protection Impact Assessments & Prior Consultation. 2019.

General Data Protection Regulation – GDPR.

GOMES**,** Maria Cecília Oliveira. Relatório de Impacto a Proteção de Dados Pessoais: uma breve análise da sua definição e papel na LGPD. **Revista AASP**, n. 144, 2019.

GOMES, Maria Cecília Oliveira. Desafios da Regulamentação do Relatório de Impacto. **jota-info**, 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/desafios-da-regulamentacao-do-relatorio-de-impacto-11022021.

ICO. PRIVACY IMPACT ASSESSMENT HANDBOOK. VERSION 2. 2009. **Huntonprivacyblog.** Disponível em:

https://www.huntonprivacyblog.com/wpcontent/uploads/sites/28/2013/09/PIAhandbookV2.pdf.

KLOZA, Dariusz *et al.* (2017). **Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals.**

Lei Geral de Proteção de Dados Pessoais.

PONTES DE MIRANDA, Francisco Cavalcanti. **História e Prática do Habeas Corpus**. 2. ed. José Konfino, 1955.

PRIVACY IMPACT ASSESMENT AND RISK MANAGEMENT. **Trilateral Research & Consulting,** 2013.

STURARI, Matheus. O DPIA na LGPD: interpretação nacional ou banalização do instrumento? Perfil do **Linkedin**, Publicado em 29 de outubro de 2020. Disponível em: https://www.linkedin.com/pulse/o-dpia-na-lgpd-interpreta%C3%A7%C3%A3o-nacional-ou-banaliza%C3%A7%C3%A3o-do-matheus/.

TANCOCK, David; PEARSON,Siani; CHARLESWORTH, Andrew. **The Emergence of Privacy Impact Assessments**. 2010.

THE EU SHOULD REGULATE AI ON THE BASIS OF RIGHTS, NOT RISKS**. Access Now**, 17 de fevereiro de 2021. Disponível em: https://www.accessnow.org/eu-regulation-ai-risk-based-approach/.

WP29, "STATEMENT OF THE WP29 ON THE ROLE OF A RISK-BASED APPROACH IN DATA PROTECTION LEGAL FRAMEWORKS"**.** 2014.

WP29. GUIDELINES ON DATA PROTECTION IMPACT ASSESSMENT (DPIA) AND DETERMINING WHETHER PROCESSING IS "LIKELY TO RESULT IN A HIGH RISK" FOR THE PURPOSES OF REGULATION 2016/679. 2017.

ZANATTA, Rafael; A.F. **Proteção de dados pessoais como regulação de risco**: uma nova moldura teórica? (2017). Artigos Selecionados REDE 2017. I Encontro da Rede de Pesquisa em Governança da Internet.

TUTELA COLETIVA E DADOS PESSOAIS

COLLECTIVE GUARDIANSHIP AND PERSONAL DATA

MARTA PRADO DE ALBUQUERQUE SEBASTIÃO[1]
VINICIUS DE MELO ALVES[2]

SUMÁRIO: 1. INTRODUÇÃO. 2. O QUE SIGNIFICA TUTELAR COLETIVAMENTE? 3. DADOS PESSOAIS PODEM SER TUTELADOS COLETIVAMENTE? 4. PARTES ENVOLVIDAS EM UMA AÇÃO COLETIVA DE PROTEÇÃO DOS DADOS PESSOAIS. 5. EXEMPLOS NO BRASIL DE MEDIDAS ADMINISTRATIVAS E AÇÕES COLETIVAS COM O OBJETIVO DE PROTEGER DADOS PESSOAIS. 6. PROPOSIÇÕES CONCLUSIVAS. REFERÊNCIAS BIBLIOGRÁFICAS

RESUMO

O presente artigo faz uma breve análise sobre as tutelas coletivas e dados pessoais, partindo de considerações sobre o contexto histórico na formação das tutelas coletivas e sua importância no Brasil, além de explicitar conceitos e classificações básicas sobre o microssistema dos direitos coletivos. Também apresenta o rol de legitimados para a propositura das ações coletivas previstos em leis ordinárias nacionais e dá exemplos da ação preventiva e repressiva destes autores e representantes no âmbito nacional posterior a 2015, tendo como panorama a Lei Geral de Proteção de Dados vigente. A problemática enfrentada pela pesquisa é: os dados pessoais podem ser tutelados coletivamente? Se sim, quais seriam os legitimados para a propositura? Existem exemplos atuais? Conclui-se que os dados pessoais podem ser tutelados coletivamente, principalmente, em determinadas situações, a proteção desses dados pode ser caracterizada como um direito essencial para muitas pessoas, e até mesmo para a sociedade como um todo. A pesquisa foi realizada pela técnica da pesquisa bibliográfica, análise de mídias e de artigos sobre a temática, além da legislação nacional, na qual os principais conceitos foram explorados para se atingir o objetivo almejado.

Palavras-chave: Tutela coletiva dos dados pessoais; Lei Geral de Proteção de Dados (LGPD); Dados pessoais; Direito Digital; Tutela coletiva.

ABSTRACT

[1]Advogada, Encarregada de Dados, Analista de Compliance, Bacharel em Direito pela Faculdade de Direito de Sorocaba. Pós-graduanda em Direito Digital e Compliance pela Faculdade IBMEC São Paulo.
[2]Advogado, Bacharel em Direito pela Faculdade de Direito de Sorocaba.

This article presents an analysis of collective protections and personal data, starting from considerations about the historical context in the formation of collective protections and their importance in Brazil, in addition to explaining basic concepts and classifications about the microsystem of collective rights. It also presents the list of legitimized for the purpose of the collective actions provided for in national common laws and gives examples of the preventive and repressive action of these authors and representatives at the national level after 2015, having as an overview the General Data Protection Law in force. The problem faced by the research is, can personal data be collectively protected? If so, what would be the legitimized for the purpose and collective? Are there current examples? It concludes that personal data can be collectively protected, especially in certain situations, the protection of such data be characterized as an essential right for many people, and even for society as a whole. The research was carried out by the technique of bibliographic research, media analysis and articles on the theme, in addition to the national legislation, in which the main concepts were explored to achieve the desired objective.
Keywords: Collective guardianship of personal data; General Data Protection Act (LGPD); Personal data; Digital Law; Collective guardianship.

1 INTRODUÇÃO

Neste trabalho será abordado inicialmente o breve panorama histórico das tutelas coletivas no Brasil, o conceito de tutela coletiva dos dados pessoais, os legitimados para a propositura das ações que versam sobre direitos difusos, coletivos e individuais homogêneos, inclusive com exemplos dessas tutelas no Brasil e, de forma mais específica, os relacionados à proteção de dados pessoais.

A relevância do tema em questão está em sua atualidade e na necessidade social brasileira pela proteção de forma coletiva, visando também aumentar a eficiência no cumprimento das leis e o equilíbrio entre as relações sociais. Ainda mais, quando tutelar coletivamente for ato essencial à proteção dos dados pessoais, como será abordado, tal defesa não terá reflexo apenas na esfera individual.

Ao longo do artigo serão respondidas as seguintes questões: o que significa tutelar coletivamente? Os dados pessoais podem ser tutelados em prol de toda uma coletividade? Quais são as entidades e pessoas legitimadas para propor uma ação que visa proteger dados pessoais de indivíduos determinados, determináveis ou indetermináveis? Há exemplos atuais

no Brasil desta tutela transindividual de proteção de dados pessoais, tendo em vista a vigência da Lei Geral de Proteção de Dados (Lei n. º 13.709/2018)?

O objetivo é trazer esclarecimentos sobre esse tema pouco explorado, haja vista a contemporaneidade da temática e a correlação entre os dados pessoais, muitas vezes vistos no prisma unicamente individual, e também sobre a proteção de maneira coletiva desses direitos inerentes à pessoa humana.

O método utilizado para alcançar tal objetivo é o hipotético-dedutivo. Além disso, serão utilizadas pesquisas documentais e bibliográficas, artigos, entrevistas e palestras em renomados canais de mídia, e principalmente leis presentes no ordenamento jurídico brasileiro.

A estrutura do presente artigo científico apresenta a construção do conhecimento e da compreensão sobre o tema, de modo a ter como partida conceitos iniciais, como quais são as formas e os possíveis motivos de tutelar coletivamente, quem são os legitimados, com contextualização e exemplos, e a partir desse conhecimento serão encontrados temas que usarão o previamente exposto, e assim sucessivamente serão abordadas situações mais complexas que envolvem os temas tutela coletiva e proteção de dados.

2 O QUE SIGNIFICA TUTELAR COLETIVAMENTE?

Com o decorrer do tempo e após diversos conflitos sociais, iniciou-se a formulação e consolidação de uma ideia, a qual estabelecia a todos indivíduos uma parcela de direitos considerada essencial para a vida em sociedade. Também, foi criado um mecanismo de proteção à ordem social e uma certa forma de controle de situações que desequilibram a sociedade como um todo.

Nota-se, ao analisar momentos passados, que sempre existiram grupos dominantes e grupos vulneráveis na sociedade. A partir da implantação do regime democrático, as medidas para o estabelecimento da defesa aos direitos fundamentais foram mais concretas, gerando proteção aos grupos ou aos indivíduos mais vulneráveis (por condição ou situação), considerando-se também a repercussão geral de determinadas situações.

Inclusive, com a iminente possibilidade de ocorrerem situações não admitidas pela sociedade e diante do poder de situações ou indivíduos de desestabilizarem ou atingirem toda a sociedade, em máxima desvantagem perante o agressor, por vezes, necessitando até a intervenção de um terceiro, foi necessário agir em prol da defesa dos direitos coletivos em sentido amplo.

Ademais, a iniciativa, que poderia partir de terceiro para proteger aquele que não tem consciência da ameaça aos seus direitos, é também uma das bases da ideia de defesa de direitos através das formas coletivas.

Nesse sentido, a tutela dos direitos coletivos é uma tentativa social de busca por defesa além da esfera individual, com fundamento em direitos conquistados pelo acordo social, estabelecidos também na CRFB/88, como o direito à vida, à liberdade, à igualdade, à segurança e à propriedade (art. 5º, da CRFB).

Ainda, os atos do Poder Público também estão sujeitos a violações aos direitos coletivos, por isso, também é necessário observar se os atos são de fato uma forma de representar a sociedade e o seus anseios, e não apenas o de exercer domínio irrestrito sobre a população.

Com relação aos direitos coletivos em sentido amplo, para facilitar a compreensão, eles são divididos em categorias pela lei, como: direitos difusos, coletivos e individuais homogêneos, dispostos no art. 81 da Lei n. º 8.078/90 (Código de Defesa do Consumidor).

Os direitos difusos são aqueles que não têm titulares determinados e que não são possíveis de serem determinados, pois têm como vítima os indivíduos e toda a sociedade ao mesmo tempo, estes ligados por um fato, cujo objeto atingido não pode ser dividido.

Já os direitos coletivos, em sentido estrito, têm como titulares um conjunto de pessoas, que pertencem a um grupo, classe ou categoria, ligados por relação jurídica, como o direito criado pela lei ou por contratos. Podem ter como partes do conflito as pessoas do conjunto ou o conjunto de pessoas e o violador dos direitos.

Por fim, os direitos individuais homogêneos, que podem também ser tutelados por meio de uma ação individual, mas que, por conveniência, facilidade no acesso e economia processual, podem ser exercidos de maneira coletiva. A classificação do direito como "homogêneo" advém da origem do direito, que é o fato que liga essas várias pessoas.

Assim como o conceito de direitos coletivos, o conceito de tutela coletiva também abarca um gênero amplo, que envolve a proteção de maneiras diversas, que, quando abordado sobre o ponto de vista jurídico, com foco na proteção das pessoas da sociedade em diversas situações, por meio judicial ou extrajudicial, passa a ser denominado de tutela coletiva.

A tutela de um direito coletivo se dá quando o direito protegido pertence a uma gama de pessoas, que por sua vez podem até não ter pleiteado a tutela, como por exemplo nos direitos difusos e coletivos.

Além disso, deve-se diferenciar tutelas coletivas de direitos, que são formadas apenas para defender direitos individuais que se transformam em coletivos por haver repercussão coletiva. Nesse sentido, diferencia-se também a ação coletiva por versar sobre a tutela de uma coletividade. Os conceitos parecem muito próximos, porém se diferenciam também por sua abrangência e aplicabilidade.

A partir da exposição feita neste capítulo, que abarca diversos conceitos e aplicações da ferramenta que é a defesa de direitos pela forma coletiva, é possível questionar: os dados pessoais, muitas vezes focados em apenas um indivíduo e na repercussão individual, são passíveis de proteção de forma coletiva? Essa será a questão abordada no item a seguir.

3 DADOS PESSOAIS PODEM SER TUTELADOS COLETIVAMENTE?

Sim, o direito à proteção dos dados pessoais, garantido na Lei Geral de Proteção de Dados (LGPD), apesar de abordar o direito que tende a ser puramente individual, abarca também outros direitos e outras possibilidades, que nem sempre podem ser separados do direito à proteção aos dados pessoais.

Um exemplo dessa situação ocorre quando um indivíduo tem direito a ter sua privacidade respeitada, porém um site de compras começa a disponibilizar seus dados pessoais na internet para todos os usuários. Inicialmente, o direito à proteção dos dados pessoais é individual, porém, se for descoberto no decorrer do processo que a prática de "vazamento" era comum, os atos de vazamento e disponibilização atingem de forma negativa toda a segurança social.

Também é possível mencionar que o direito à proteção de dados pessoais inclui assuntos sensíveis à sociedade, como a proteção da criança e do adolescente. Para exemplificar, quando um site permite o tratamento de dados pessoais de adolescentes de forma contrária às leis brasileiras, há lesão a direitos que podem ser classificados como direitos difusos, ou, quando é possível identificar os adolescentes envolvidos, poderão ser classificados como direitos coletivos em sentido estrito (art. 227, da CRFB/88 e art. 14, da LGPD).

Em complemento à importância da proteção dos dados pessoais, há um conceito exposto pelo escritor Eli Pariser que, em 2011, em uma apresentação do *TED talk*[3], expôs o

[3]PARISER, Eli. Tenha cuidado com os "filtros-bolha" online. TED Talks, 2011. Disponível em: https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles/transcript?language=pt-br. Acesso em: 16 set. 2020.

conceito de *Filter Bubbles* (“Bolhas Sociais”), isto é, a separação de pessoas, dentro de seus gostos, com base no tratamento de dados, que com o tempo poderiam afetar o comportamento humano e, por consequência, todo o equilíbrio social, inclusive aumentando preconceitos e distorções sociais.

O conceito de *Filter Bubbles* (“Bolhas Sociais”) permite observar a necessidade do acesso à informação e compreensão dos titulares dos dados, para que exerçam também seus direitos e anseios sociais em meio digital, combatendo: a “perseguição da publicidade”, a ditadura dos dados, a manipulação, o aproveitamento das vulnerabilidades, a legítima expectativa, o estabelecimento e o uso sem limites dos perfis criados com bases nos dados, e a programação neurolinguística irrestritamente utilizada.

Dessa forma, a não repetição de preconceitos e mazelas sociais pelo tratamento inadequado dos dados pessoais também podem ser considerados um direito difuso, pois ferramentas atuais, como a Inteligência Artificial, podem ter um banco de dados tendencioso e implementado para determinado fim.

De forma sucinta, podem ser inseridos em uma máquina que utilize Inteligência Artificial registros históricos preconceituosos, como parâmetros a serem replicados, e com a ampliação do uso e das possibilidades oferecidas pela internet, não será difícil a dispersão de informações manipuladas ou mesmo o uso desses recursos como mecanismo de seleção social.

Assim, o Estado, como representante dos anseios sociais, deverá proteger não só os indivíduos, quando o assunto é proteção de dados pessoais, mas proteger a sociedade como um todo, regulando e fiscalizando as práticas, além de permitir que todos os meios de proteção sejam utilizados, quando adequados.

Observa-se também que não é incomum a utilização de dados pessoais, como moeda de troca e ganho financeiro, não sendo somente direitos, como a privacidade, invadidos, mas também a própria economia. Assim, os dados pessoais também têm potencial de reconstituir o indivíduo e seus gostos, sendo comercializado o próprio ser humano.

Nesse sentido, também são necessárias as tutelas coletivas para que as leis que abordem o tema *proteção de dados pessoais* não afetem negativamente outros direitos fundamentais, como a liberdade de expressão, a dignidade da pessoa humana ou direito à ordem econômica.

Ademais, com relação às relações de consumo, ressalta-se a Teoria do Risco, a qual estabelece que o fornecedor do serviço deverá arcar com os riscos da atividade, ou seja,

assume-se a responsabilidade ao tratar de dados pessoais, inclusive diante de uma ação coletiva.

Também, um cenário de previsão discutido atualmente é a possibilidade de abordar de forma coletiva o uso de Inteligência Artificial (IA) no judiciário[4], por conta de decisões feitas por "máquinas" e da relação entre bancos de dados desatualizados ou utilizados de forma arriscada pela Justiça.

Contudo, os riscos do tratamento inadequado dos dados pessoais podem ser controlados, principalmente pelo Estado, a fim de representar os anseios sociais, inclusive medindo suas próprias ações.

Assim, os dados pessoais podem ser tutelados coletivamente e são amparados pela CRFB/88, pela LGPD, Código de Defesa do Consumidor, Lei de Ação Civil Pública, dentre outras, que fundamentam a proteção de dados pessoais, por meio judicial ou extrajudicial.

A consciência social sobre o tema e o exercício dos direitos são atitudes iniciais para o uso das ferramentas de proteção coletiva, e que devem ser acompanhadas também do treinamento dos agentes de tratamento dos dados pessoais. Nesse sentido, uma opção é a implementação do *compliance* (ação em conjunto pela observância das regras, diretrizes, leis).

Em suma, é possível que os dados pessoais sejam tutelados coletivamente, em razão da importância social que eles exercem, por conta da probabilidade de afetarem não só o indivíduo, mas toda a sociedade, e também pela necessidade, em alguns contextos, de ações no sentido de proteger grupos de indivíduos em situação de vulnerabilidade.

Nesse sentido, para conhecer mais sobre as formas de tutelar coletivamente os dados pessoais e sobre o próprio direito de proteção, o próximo item trará solução à questão: quais são as partes envolvidas em uma ação coletiva de proteção dos dados pessoais?

4 PARTES ENVOLVIDAS EM UMA AÇÃO COLETIVA DE PROTEÇÃO DOS DADOS PESSOAIS

No âmbito da ação coletiva, é possível citar exemplos de peças processuais, como a ação civil pública, a ação civil coletiva, o mandado de segurança coletivo, entre outras, presentes em leis esparsas. Já que não há um código de processo coletivo, as normas que

[4]BREHM, Katie, *et al* . O futuro da IA no sistema judiciário brasileiro. Apêndice, páginas 44/47. ITS Rio, 2020. Disponível em: https://itsrio.org/wp-content/uploads/2020/07/TRADUC%CC%A7A%CC%83O-The-Future-of-AI-in-the-Brazilian-Judicial-System.pdf. Acesso em: 16 set. 20.

possuem um arcabouço mais substancial sobre o tema são a Lei n. º 8.078/90 (Código de Defesa do Consumidor) e a Lei n. º 7.347/85 (Lei de Ação Civil Pública).

A LGDP manteve-se silente ao não delimitar os legitimados ativos para a tutela de direitos transindividuais nos arts. 22 e 42, §3º, que abordam o tema (de forma) metaindividual. Entretanto, imputou aos operadores e aos controladores a solidariedade na responsabilização de danos causados, seja na lesão individual ou coletiva, havendo um pequeno rol de exclusão de responsabilidade, presente no art. 43.

Ressalta-se a aplicação de sanções administrativas disposta na LGPD, que definiu o Fundo de Defesa de Direitos Difusos como beneficiário das multas aplicadas pela ANPD, citando explicitamente a Lei de Ação Civil Pública, em seu texto legal (Art. 52, §5º, da LGPD), superando qualquer ideia de exclusiva individualidade que ela tutela.

Usualmente, e aplicando-se à tutela coletiva dos dados pessoais da mesma maneira, a Lei de Ação Civil Pública, em seu 5º artigo, define como legitimados ativos (I) o Ministério Público, (II) a Defensoria Pública, (III) a União, os Estados, o Distrito Federal e os Municípios, (IV) a autarquia, empresa pública, fundação ou sociedade de economia mista e (V) a associação legalmente constituída há pelo um ano com pertinência temática do direito a ser tutelado. Por interpretação analógica e em decorrência do princípio da subsidiariedade, não havendo vedação da LGPD, os mesmos parágrafos se aplicam no caso da tutela coletiva dos dados pessoais.

O artigo 82, III, do Código de Defesa do Consumidor, também prevê a possibilidade de entidades e órgãos da Administração Pública, mesmo os despersonalizados, de promoverem a defesa de interesses e direitos previstos na lei (Ex. Procon).

Precipuamente, o Ministério Público possui o dever institucional da proteção dos interesses sociais, individuais indisponíveis, difusos e coletivos, conforme previsto no art. 127, *caput* e art. 129, III, da Carta Constitucional. Além de previsão constitucional e institucional propriamente dita, a Lei de Ação Civil Pública (Art. 5º, §1º) e o CDC (art. 92) determina que se o Ministério Público não atuar como parte, intervirá como fiscal da lei. Em síntese, o interesse que o Ministério Público possui na tutela da coletividade é decorrente da lei e compõe seu próprio fim institucional. Se o bem é difuso ou coletivo, poderá ser protegido pelo *Parquet*.

Quanto à Defensoria Pública (art. 134, CRFB), há uma peculiaridade no amparo dos hipossuficientes, a qual André Roque transmite de maneira clara e objetiva[5].

Quanto à motivação dos entes políticos para a tutela coletiva, poderá ser amplamente visualizada pela manifestação dos órgãos, entidades e divisões, como os Procons, a Secretaria Nacional do Consumidor (Senacon), o Departamento de Defesa e Proteção do Consumidor (DPDC), e a Coordenação de Consumo e Sociedade da Informação (CCSI).

Ainda, Marcelo Sodré explica que a criação da Senacon, em 2012, ocorreu pela visão mais ampliada da relevância do direito do consumidor, na atual onda neoconstitucional, e na "criação de um sistema de repressão de violações à ordem econômica e aos direitos básicos dos consumidores"[6]. Para Rafael Zanatta e Michel Souza, a determinação de competência para a CCSI foi de suma importância para a LGDP[7].

Por último, mas não menos importante, a Lei n. º 7.347/85 (Lei de Ação Civil Pública) prevê, no rol de legitimados ativos, as associações civis, desde que constituídas há um ano e com pertinência temática sobre o assunto a ser tutelado[8].

Uma organização não governamental, para tutelar os dados pessoais ou para a proteção dos consumidores, poderá ser criada como forma de fiscalizar empresas de uma determinada cidade, logicamente com a visão de proteção dos dados individuais. Inclusive, caso alguma

[5]A Defensoria Pública também possui legitimidade ampla, desde que a questão envolva potencialmente o interesse de hipossuficientes – não sendo necessária, todavia, a comprovação de que apenas hipossuficientes sejam beneficiados.# Desse modo, a Defensoria Pública poderia atuar em juízo, por exemplo, genericamente na defesa dos interesses de clientes de uma companhia telefônica, mas não em defesa dos consumidores de uma marca de automóveis de luxo. ROQUE, André. *A Tutela Coletiva dos Dados Pessoais na Lei Geral de Proteção de Dados Pessoais (LGPD).* Revista Eletrônica de Direito Processual – REDP. Rio de Janeiro. Ano 13. Volume 20. Número 2. Maio a agosto de 2019. Periódico Quadrimestral da Pós-Graduação Stricto Sensu em Direito Processual da UERJ.

[6]SODRÉ, Marcelo. *A formação do Sistema Nacional de Defesa do Consumidor*. São Paulo: RT, 2007.

[7]"(...) [A CCSI] teria como competência 'realizar estudos e análises técnicas relacionados ao comércio eletrônico, proteção da privacidade e dados pessoais do consumidor e demais temas relacionados à sociedade da informação, para propor medidas preventivas e repressivas a infrações às normas de defesa do consumidor' (art. 25, I) e 'desenvolver ações para promover o constante acompanhamento da utilização de dados pessoais no mercado de consumo e coibir eventuais abusividades' (art. 25, III). Criou-se, assim, a base jurídica para um trabalho mais sofisticado de investigações em proteção de dados pessoais e para coibir abusividades (...). O enfoque da Senacon em proteção de dados pessoais, explicitado em 2012, reflete-se também no papel que a Secretaria teve, junto ao Ministério da Justiça, na estruturação da consulta pública ao Anteprojeto de Lei de Proteção de Dados Pessoais.# Além disso, nota-se o papel que especialistas em proteção de dados pessoais ocuparam na Secretaria. ZANATTA, Rafael; SOUZA, Michel. A tutela coletiva em proteção de dados pessoais: Tendências e desafios. 2019 p. 24).

[8]Nesse sentido: "As associações civis necessitam, portanto, ter finalidades institucionais compatíveis com a defesa do interesse transindividual que pretendam tutelar em juízo. Entretanto, essa finalidade pode ser razoavelmente genérica; não é preciso que uma associação civil seja constituída para defender em juízo especificamente aquele exato interesse controvertido na hipótese concreta. (...) Essa generalidade não pode ser, entretanto, desarrazoada, sob pena de admitirmos a criação de uma associação civil para a defesa de qualquer interesse, o que desnaturaria a exigência de representatividade adequada do grupo lesado" (STJ, AgRg no REsp 901.936, 1ª T., Rel. Min. Luiz Fux, julg. 16.10.2008).

empresa não cumpra as normas, a própria associação civil pode ajuizar uma ação coletiva com o fim de coibir ou requerer o ressarcimento dos danos causados pelo descumprimento da norma e forma de tratamento dos dados.

Após a exposição de exemplos da lei sobre quem pode ser legitimado ativo na tutela coletiva de direitos, deve-se acrescentado que, com relação a quem ocupa o polo passivo, não há restrição legal. Além disso, a instituição ou pessoa que ferir, ameaçar difusa ou coletivamente, ou lesar os cidadãos, criando uma relação metaindividual, característica deste microssistema, poderá ser parte ré na ação, inclusive se algum dos legitimados ativos for o infrator, podendo ocupar o polo passivo da demanda. Neste aspecto, aplica-se a parte geral de processo, no que tange à triangulação da relação litigiosa.

Por fim, conclui-se que se a LGPD for interpretada por um viés unicamente de tutela individual, certamente se perderá um grande debate sobre a efetividade da proteção em si, tendo em vista a enorme abrangência e repercussão que a tutela transindividual causa sobre a sociedade, seja de maneira consciente ou inconsciente de seus membros.

5 EXEMPLOS NO BRASIL DE MEDIDAS ADMINISTRATIVAS E AÇÕES COLETIVAS COM O OBJETIVO DE PROTEGER DADOS PESSOAIS

Observando de um prisma futurista e preventivo das lides iminentes de dados pessoais de toda uma coletividade, surgem então dúvidas: o que esperar dos legitimados ativos quando se trata de lesão ou danos aos dados pessoais? Há exemplos na atualidade da aplicação meta individual da tutela coletiva de dados pessoais? Em resposta a estes questionamentos, André Roque dá exemplos práticos quando os direitos podem ser tutelados coletivamente.

Há outros exemplos de medidas mais rebuscadas e com soluções mais difíceis decorrentes da possibilidade de mudanças de análise estrutural e tratamento.

Neste plano abordado, a ideia da violação seria apenas em hipótese, pois a prevenção, quando bem realizada, evita diversos conflitos, seja para indivíduos indetermináveis, ligados por uma situação de fato (difusos) ou indivíduos determináveis de uma categoria ou classe, ligados por uma relação jurídica base (coletivo em sentido estrito).

Diante disso, atitudes de educação e conscientização sobre o uso de dados, o *compliance* dos controladores e operadores, a publicidade clara sobre como os dados serão utilizados, e outras inúmeras ideias, podem surgir de acordo com as necessidades crescentes e da atual precisão da boa-fé objetiva.

A própria ação civil pública, no inquérito civil (Art. 8º LACP), o termo de ajustamento de conduta (TAC) são instrumentos criados pela lei para balizar e legitimar as ações, principalmente preventivas, mas também remediativas, na efetividade da aplicação do direito individual da tutela coletiva e da proteção dos dados pessoais.

O primeiro caso exemplificativo é de uma das gigantes de telefonia (Oi) que, em conjunto com uma empresa britânica, desenvolveu um software denominado "Navegador", que mapeava o tráfego de dados do consumidor na internet de modo a criar um perfil de navegação.

No Brasil, mesmo antes da vigência da LGPD, o Ministério Público do Distrito Federal e Territórios (MPDFT) criou uma unidade especial de proteção de dados pessoais, coordenada pelo promotor de justiça criminal, Frederico Meinberg Ceroy. O sítio eletrônico do MPDFT contém os sete pilares de atuação da comissão que também desempenha um importante papel na proteção dos dados pessoais da seguinte maneira: Pilar Opinativo, Pilar Informativo, Pilar de Estudos, Pilar de Cooperação, Pilar de Notificação, Pilar Sancionador e Pilar Investigativo.[9]

É possível ver um quadro comparativo de vazamento de dados e danos coletivos causados aos brasileiros, desenvolvido pelo escritório Azevedo Sette em janeiro de 2019, que demonstra a atuação proativa que o MPDFT já teve.[10]

Após a exposição acima, fica clara a importância da atuação do Ministério Público e de outros órgãos para a proteção e defesa dos consumidores em prol da coletividade.

De maneira muito semelhante, as associações civis e organizações não governamentais atuam na proteção dos dados pessoais sensíveis ou não sensíveis dos brasileiros. O Instituto Brasileiro de Defesa do Consumidor (IDEC) moveu uma Ação Civil Pública em face da empresa *ViaQuatro*, uma das concessionárias do metrô da cidade de São Paulo. Isto porque a concessionária tinha a pretensão de instalar um sistema de Portas Interativas Digitais, com

[9]Um dos casos emblemáticos trata da abertura do procedimento preparatório em face da Uber do Brasil Tecnologia Ltda. por conta de um incidente de segurança ocorrido em meados do final de 2016, quando houve invasão do sistema e violação de informações de usuários, tanto clientes como motoristas. O objetivo do procedimento é investigar as circunstâncias e as causas do referido incidente, bem como apurar as responsabilidades pelos danos causados#. Além desse caso, foram abertos inquéritos civis para apuração de responsabilidade pelo vazamento de dados de outras pessoas jurídicas, tais como Federação das Indústrias de São Paulo (FIESP) (...) Nesse acordo, chama atenção a postura do MPDFT de ressaltar "a necessidade de incentivar as empresas, vítimas de incidentes de segurança, a optarem por colaborarem com as investigações do Ministério Público em detrimento do pagamento de quantia aos autores dos incidentes com o objetivo de ocultar o acontecido". (ZANATTA, Rafael; SOUZA, Michel. *A tutela coletiva em proteção de dados pessoais: Tendências e desafios*. 2019, p. 27-28).

[10]Disponível em: http://www.azevedosette.com.br/noticia/atuacao-sistematica-do-mpdft/5225

capacidade de captar a reação das pessoas diante delas, além de contar o número de usuários que teriam contato com o conteúdo mostrado.

Nesse exemplo, foi realizado um questionamento sobre a legalidade do registro de imagens e expressões faciais dos usuários do metrô, e a identificação das emoções dos passageiros diante de peças publicitárias[11]. A decisão cautelar foi favorável ao Instituto e determinou a suspensão do funcionamento das portas interativas sob pena de multa, sendo que ainda está em trâmite processual.

Após analisar todos estes exemplos e os muitos outros que surgirão em um futuro próximo, nota-se a eminente e contínua ação por parte dos legitimados na proteção coletiva do direito individual dos dados pessoais. Ao mesmo tempo que uma certa "paz de consciência" inunda o espírito humano ao saber que há entidades agindo para assegurar a individualidade, não discriminação e privacidade dos cidadãos, o temor e o receio também dissolvem esse mesmo espírito à medida que a indústria da tecnologia, cada vez mais ávida em evoluir, busca também enriquecer, muitas vezes de maneira ilícita, aproveitando-se da ausência de conhecimento técnico dos indivíduos e usuários.

6 PROPOSIÇÕES CONCLUSIVAS

Com base nas informações apresentadas no presente artigo, é possível concluir que o tema tratado é de alta relevância social, pois envolve situações e indivíduos de forma que suas ações refletem também nos demais indivíduos presentes na sociedade.

Assim, como reflexo de atitudes realizadas em detrimento da harmonia nas relações entre os indivíduos e opostas aos preceitos estabelecidos pelo coletivo em leis, foi criado progressivamente, o conceito de uma suposta tutelar coletivamente.

Portanto, ressaltou-se, com ênfase, que o significado de tutelar coletivamente é proteger a sociedade e seu equilíbrio nas relações por meio de instrumentos e ferramentas judiciais e extrajudiciais.

Dessa forma, a partir do conceito deste ato de defesa em prol da sociedade, foi abordado especificamente a possibilidade do seu envolvimento com a proteção de dados

[11]SOPRANA, Paula. *Concessionária é alvo de processo por leitura facial no metrô de SP*. Folha de São Paulo. BRASIL. Tribunal de Justiça de São Paulo. Processo n. 1090663-42.2018.8.26.0100. Disponível em: https://esaj.tjsp.jus.br/cpopg/show.do?processo.codigo=2S000WSPS0000&processo.foro=100&processo.numero=1090663-42.2018.8.26.0100&uuidCaptcha=sajcaptcha_8c9f8fb8b64e4babb84be29cb5048b4bTJSP. Acesso em: 27 ago. 2020.

pessoais, especialmente amparada pela Lei Geral de Proteção de Dados, o que foi demonstrado ser possível e essencial.

Conforme foi demonstrado, os dados pessoais podem ser aplicados em diversas situações que denotam as possibilidades intrínsecas de importância social. Além disso, e em muitas delas, esses dados são acompanhados de direitos coletivos em sentido amplo (direitos coletivos em sentido estrito, direitos difusos e direitos individuais homogêneos), muitos desses são definidos também como direitos fundamentais.

Portanto, tutelar coletivamente os dados pessoais é agir em prol da sociedade, utilizando ferramentas e instrumentos, judiciais e extrajudiciais, que vêm se consolidando ao longo do tempo, como forma de exercício do poder social de proteger todos de situações desequilibradas e que, muitas vezes, demonstram elevado prejuízo aos indivíduos em situação de vulnerabilidade.

Ainda, é possível concluir que os legitimados ativos possuem uma determinação legal ao tutelar coletivamente os dados pessoais dos indivíduos. Observou-se que a Constituição Brasileira e as leis do microssistema da tutela coletiva asseguram que os legitimados representem uma coletividade, realizem ações e acordos em nome de classes, consumidores e até de cidadãos indetermináveis. Conclui-se que estes órgãos, entidades e instituições não são fins em si mesmos, mas agem de maneira preventiva e repressiva para evitar as lesões e ameaças a direitos fundamentais no âmbito dos dados pessoais.

Na atualidade, os Procons, os Ministérios Públicos, as associações com a finalidade da proteção de consumidores, atuam constantemente para preservar a autodeterminação, a individualidade, o sigilo, o consentimento, a vontade de toda uma coletividade formada por indivíduos. Não há liberdade, como um direito fundamental, sem transparência ou informação clara e objetiva, tendo em vista a era dos dados e seu preço valioso na contemporaneidade. Além disso, se a punição às instituições que não cumprem a Lei Geral de Proteção de Dados não tiver, além do caráter ressarcitório, o caráter pedagógico, dificilmente sua cultura e a dos agentes de tratamento de dados será modificada no que tange ao respeito ao indivíduo.

Por fim, a disseminação do conhecimento sobre como os dados pessoais de uma massa podem ser tutelados coletivamente foi iluminada, tornando-se um incentivo para a busca de mais informações sobre a temática, bem como que esse conhecimento se torne uma ferramenta para inibir atos contra a dignidade da pessoa humana no âmbito dos dados pessoais.

REFERÊNCIAS BIBLIOGRÁFICAS

BASTOS, Athena. **Direitos e garantias fundamentais**: o que são e quais as particularidades. SAJADV, publicado em 2018, atualizado em 2020.

BASTOS, Fabrício. Nomenclaturas Básicas na Tutela Coletiva. **Youtube**, 2020.

BLUM, Rita Peixoto Ferreira. **O Direito à Privacidade e à Proteção dos Dados do Consumidor.** São Paulo: Almedina, 2018.

BRASIL. **Ministério da Justiça e Segurança Pública**. Senacon instaura processo contra a Google Brasil, 07/02/2019.

BRASIL. **Tribunal de Justiça.** Ministério da Justiça multa Oi por monitorar navegação de consumidores na internet.

BRASIL. São Paulo. Atuação Sistemática do MPDFT. **Azevedo Sette Advogados**.

COSSETTI, Melissa Cruz. **O que é inteligência artificial**. Tecnoblog.

DANTAS, Rosalliny Pinheiro. **O mandado de segurança coletivo.** Âmbito Jurídico, 2012.

FOLHA DIRIGIDA. Entenda o impacto da LGPD no setor público. Canal Folha Dirigida, **YouTube**, 2019.

GAIZO, Flavia Viana Del. **Evolução histórica das ações coletivas:** enfoque especial para o surgimento das ações coletivas passivas. PUC SP, 2017.

GASTALDI, Suzana. **Direitos difusos, coletivos em sentido estrito e individuais homogêneos:** conceito e diferenciação. Âmbito Jurídico, 2014.

GODOY, Paulo Henrique Silva. Tutela coletiva. Defesa do consumidor em juízo. **YouTube,** 2017.

GONÇALVES, Marcus Vinicius Rios. **Tutela de interesses difusos e coletivos**. 10. ed. São Paulo: Saraiva, 2016. Livro Digital. (Sinopses jurídicas, 26"). ISBN 9788547203818. Disponível em: https://integrada.minhabiblioteca.com.br/books/9788547203818. Acesso em: 27 ago. 2020.

ITS RIO. Suas buscas na Internet podem aparecer em um inquérito? Canal ITS Rio, **YouTube,** 2019.

MARTINS, Thais Macedo. **Tutela coletiva e estado democrático de direito.** Relações com o direito do trabalho. Publica Direito.

PARISER, Eli. Tenha cuidado com os "filtros-bolha" online. TED Talks, 2011.

PORTAL DE DIREITOS COLETIVOS. O que são Direitos Coletivos?

RIBEIRO, Flávia Pereira Ribeiro. Conceito e análise da repercussão geral. CNMP. **Jusbrasi**l, 2011. Disponível em: https://www.jusbrasil.com.br/processos/nome/32928055/flavia-pereira-ribeiro. Acesso em: 27 ago. 2020.

ZANATTA, Rafael. A tutela coletiva na proteção de dados pessoais. **Revista do Advogado**, v. 39, n. 144, nov. 2019.

APLICAÇÃO DA LEI Nº 13.709 DE 14.08.2018 E O DIREITO AO ESQUECIMENTO NOS DADOS DE NEGATIVAÇÃO SOB A ÉGIDE DO CÓDIGO DE DEFESA DO CONSUMIDOR

APPLICATION OF LAW No. 13.709 OF 08.14.2018 AND THE RIGHT TO FORGET IN THE NEGATIVE DATA UNDER THE AGENDA OF THE CONSUMER DEFENSE CODE

MARIA LUIZA RUIZ ORFALI[1]

SUMÁRIO: 1. INTRODUÇÃO. 2. SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS. 3. O DIREITO AO ESQUECIMENTO NO CAMPO DO DIREITO DIGITAL. 4. O DIREITO AO ESQUECIMENTO NA LEGISLAÇÃO BRASILEIRA E AS INOVAÇÕES TRAZIDAS PELA LGPD. 5. DIREITO AO ESQUECIMENTO NAS RELAÇÕES CONSUMERISTAS. 6. RELATIVIZAÇÃO DO DIREITO À INFORMAÇÃO EM FUNÇÃO DO DIREITO AO ESQUECIMENTO. 7. O "SCORE" COMO PRÁTICA MANIFESTAMENTE ABUSIVA. 8. CONCLUSÃO. REFERÊNCIAS BIBLIOGRÁFICAS.

RESUMO

A Lei Geral de Proteção de dados impactou os mais diversos ramos do direito no ordenamento jurídico brasileiro. O presente estudo visa discutir os impactos do referido dispositivo, especialmente em seu art. 52, na legislação consumerista, bem como a incidência do instituto do direito ao esquecimento neste.

Palavras-chave: Direito ao esquecimento; LGPD; Score.

ABSTRACT

The General Data Protection Law impacted the most diverse branches of law in the Brazilian legal system. The present study aims to discuss the impacts of the aforementioned device, especially in its art. 52, in consumer legislation, as well as the incidence of the institute of the right to be forgotten in it.

Keywords: Right to be forgotten; LGPD; Score.

1 INTRODUÇÃO

Entende-se por direito ao esquecimento a possibilidade de o indivíduo requerer que determinado fato concernente à sua vida pessoal seja "deletado" da memória coletiva para evitar constrangimentos.

Embora a discussão acerca deste instituto jurídico seja recente, ela se mostra cada vez

[1]Estudante do 3º ano diurno do Curso de Graduação em Direito na Faculdade de Direito de Sorocaba.

mais relevante em vista do advento das novas tecnologias. Os dados no campo virtual geram novas formas de constrangimento para além dos mecanismos dispostos na legislação pátria, o que reitera a importância do supracitado instituto em um mundo marcado pela Revolução Técnico-científico-informacional.[2]

Ainda que o direito ao esquecimento seja comumente vinculado às áreas cível e criminal, transplantando-o ao Direito do Consumidor, surge a asserção do Direito ao esquecimento do consumidor.

Caracteriza-se tal quadro quando, apesar da ocorrência da prescrição do débito, as instituições credoras mantêm, em bancos de dados internos, a negativação do consumidor inadimplente. Esta conduta, por ferir direitos constitucionais, configura prática abusiva e entra em conflito com a LGPD (Lei Geral de Proteção de Dados).

Outrossim, reputa-se configurada uma crescente necessidade da aplicação do direito ao esquecimento no ordenamento jurídico brasileiro, principalmente no direito do consumidor, haja vista que este não pode ser constantemente perturbado pelo rastro de seu histórico financeiro.

Pretende-se, pois, discutir neste trabalho a configuração da utilização de dados prescritos mantidos em sistema interno de credores como prática abusiva do fornecedor, e a importância da Lei Geral de Proteção de Dados para tutelar o direito ao esquecimento quanto ao armazenamento destes dados.

2 SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS

Na contemporaneidade marcada pela globalização, o acentuado fluxo de circulação de informações e dados pessoais exige uma regulamentação com força normativa, pois assim pode haver a efetiva tutela dos direitos do indivíduo no que tange o universo virtual[3]

Nesse sentido, em resposta à constante adequação do Direito à realidade que se vive, surge a Lei Geral de Proteção de Dados, inspirada na GDPR (Regulamento Geral da Proteção de Dados ou *General Protection Data Regulation*), lei europeia que regula o tratamento de informações pessoais em vigor desde setembro de 2020.

Ao estabelecer regras em relação ao tratamento desses dados, a LGPD busca garantir maior controle, por parte dos usuários, sobre as ações que são realizadas com os seus dados (tanto em meios físicos quanto digitais), além de alterar a Lei 12.965 de 23 de abril de 2014,

[2]RIFKIN, Jeremy. A Terceira Revolução Industrial – Como o poder lateral está transformando a energia, a economia e o mundo. São Paulo: M. Books do Brasil, 2012.
[3]COMENTÁRIOS à Lei Geral de Proteção de Dados. São Paulo: Grupo Almedina, 2020. Livro Digital. (1 recurso online). ISBN 9788584935796.

chamada de Marco Civil da Internet.

Dispõe o art. 1° da LGPD, *in verbis*:

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

Para o referido diploma legal, configuram-se como dados pessoais, objeto dessa lei, qualquer informação relativa a uma pessoa singular identificada ou identificável. É considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social (art. 5°, Lei 13.709/2018).

O mesmo diploma legal, ao dispor sobre os fundamentos da proteção de dados pessoais elenca em seu art. 2°, I, o respeito à privacidade.

3 O DIREITO AO ESQUECIMENTO NO CAMPO DO DIREITO DIGITAL

O direito ao esquecimento é, em suma, um artifício disponibilizado pelo direito que visa dar ao cidadão a garantia do exercício de controle sobre seus próprios dados.

O instituto jurídico ganhou relevância no campo do direito digital com a decisão proferida pelo Tribunal de Justiça da União Europeia do caso Gonzáles (Processo n° C-131/12), facultando ao indivíduo pleitear aos controladores de dados o apagamento (desindexação) de *links* que contem com dados tidos como prejudiciais.

Outrossim, entende-se por direito ao esquecimento, no que tange o direito digital, a tutela da privacidade que deve ser efetivada por intermédio da possibilidade de pugnar pela desindexação de links e dados dispostos online, sob a égide da legislação de proteção de dados pessoais, de forma que seja assegurado o controle do indivíduo sob os seus dados pessoais.

4 O DIREITO AO ESQUECIMENTO NA LEGISLAÇÃO BRASILEIRA E AS INOVAÇÕES TRAZIDAS PELA LGPD

Consoante, infere-se do projeto de lei n° Lei 1.676/2015, de autoria do Deputado Veneziano Vital do Rêgo, em seu art. 3º, que:

> "o direito ao esquecimento é expressão da dignidade da pessoa humana, representando a garantia de desvinculação do nome, da imagem e demais aspectos da personalidade relativamente a fatos que, ainda que verídicos, não possuem, ou não possuem mais, interesse público".

Tomando-se como alicerce o conceito oferecido pelo abalizado jurista italiano Pietro

Perlingieri, conceituam-se os supracitados direitos da personalidade como "valor fundamental do ordenamento, e está na base de uma série (aberta) de situações existenciais, nas quais se traduz a sua incessantemente mutável exigência de tutela"[4]

Contempla-se, portanto, a dignidade humana como princípio jurídico, devendo haver a tutela do respeito à integridade física e psíquica das pessoas, a consideração pelos pressupostos materiais mínimos para viver e, por fim, o respeito pelas condições mínimas de liberdade e convivência social igualitária[5].

Dentre o rol de direitos da personalidade a serem velados pelo Estado Democrático de Direito, a Constituição Federal prevê que:

> "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" (art. 5°, inciso X, CF). Prevê, ainda, o Código Civil em seu art. 21 que "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."

Realizadas tais premissas legais, reputa-se configurado o direito ao esquecimento como reflexo do direito à privacidade.

Ao conferir solidez ao acima perfilhado, o Enunciado n° 531 proferido na VI Jornada de Direito Civil coordenada pelo Ministro Ruy Rosado de Aguiar, in verbis: "*A tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento*", podendo este ser assegurado por intermédio da tutela judicial inibitória (enunciado n° 576). Configuração inadequada;

Ao adentrar o campo de incidência da Lei Geral de Proteção de Dados e o direito ao esquecimento propriamente dito, o referido texto legal dispõe que os titulares de dados poderão realizar solicitação às empresas, por intermédio de simples requerimento, que forneçam, no prazo de 15 dias, informações referentes aos seus dados, devendo constar a indicação da origem dos dados, da finalidade do tratamento, dos critérios utilizados para coleta e tratamento, ou declaração de inexistência de dados, com fundamento nos artigos 9º, 18 e 19 da LGPD.

Ciente dos dados pessoais, aquele que é seu titular tem direito de requerer a eliminação dos dados pessoais tratados nos termos do art. 18, VI, Lei n° 13.709/2018). Excetua-se, não obstante, a exclusão mediante requerimento em hipóteses de cumprimento de obrigação legal ou regulatória pelo controlador, estudo por órgão de pesquisa, garantida, sempre que possível,

[4]PERLINGIERI, Pietro. Perfis do direito civil. Introdução ao Direito Civil Constitucional. Rio de Janeiro: Renovar, 1997.
[5]AZEVEDO, Antonio Junqueira de. A caracterização jurídica da dignidade da pessoa humana. Revista Trimestral de Direito Civil (RTDC). Rio de Janeiro: Padma, 2000. Volume 1.

a anonimização dos dados pessoais, a transferência a terceiro, desde que respeitados os requisitos de tratamento de dados ou uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados (art. 16, I a IV, Lei n° 13.709/2018).

5 DIREITO AO ESQUECIMENTO NAS RELAÇÕES CONSUMERISTAS

Assim que prescrita uma dívida cadastrada, deixa de existir obrigação legal que legitime a continuidade do armazenamento destes dados, tornando possível ao titular desses requerer sua eliminação, a fim de não prejudicar suas futuras relações jurídicas de consumo.

Tal possibilidade encontra fulcro no art. 43, § 1° do Código de Defesa do Consumidor, que prevê a necessidade do fornecedor de deletar dados referentes à negativação, após o decorrido período de cinco anos sem a execução judicial de tal dívida.

O uso desses dados após sua prescrição configura prática abusiva e desproporcional, sendo condenável pelo CDC.

Não obstante, ainda que haja expressa previsão legal, há instituições que, de forma velada, não seguem o disposto, lesando o consumidor por meio do uso e da manipulação indevida de dados[6].

Tal manipulação se dá com a manutenção de banco de dados internos que ignoram a limitação de tempo imposto pelo ordenamento jurídico e criam a restrição interna sem vinculações com possíveis inscrições nos órgãos de proteção ao crédito.

O consumidor, apenas quando lhe é negada a celebração de negócio jurídico com instituição detentora desses dados, descobre que ainda há resquícios de seu débito já prescrito.

Por ser parte insuficiente da relação, o consumidor fica subserviente ao arbítrio viciado destas instituições que podem se negar a fornecer bens e serviços.

Esse sistema interno não considera os dados já arquivados - e prescritos - que se encontram nos órgãos de proteção ao crédito, como o SPC-SERASA, penalizando o consumidor *ad infinitum*.

A existência deste banco de dados interno mostra-se contrária ao que é disposto no ordenamento jurídico brasileiro, majoritariamente oriundo dos artigos 39 e 51, inciso IV, Código de Defesa do Consumidor, e no artigo 2º, letra a da Resolução BACEN nº 1.631/89 alterada pela Resolução BACEN nº 1.682/90.

Nessa senda, o Código de Defesa do Consumidor, no artigo 39, incisos II e IX, veda, de

[6]SILVA NETO, Orlando Celso da. Comentários ao Código de Defesa do Consumidor. Rio de Janeiro: Forense, 2013. Livro Digital. (1 recurso online). ISBN 978-85-309-5039-2.

forma reiterada, ao fornecedor de produtos ou serviços, recusar atendimento às demandas dos consumidores, na exata medida de suas possibilidades e seu estoque, e, ainda, de conformidade com os usos e costumes, proibindo-se recusar a venda ou a prestação de serviços diretamente a quem se disponha a adquiri-los mediante pronto pagamento.

Ademais, em seu artigo 51, inciso IV, o CDC dispõe que "serão nulas de pleno direito, entre outras, as cláusulas contratuais relativas ao fornecimento de produtos e serviços que (…) estabeleçam obrigações consideradas iníquas, abusivas, que coloquem o consumidor em desvantagem exagerada, ou seja, incompatíveis com a boa-fé ou a equidade".[7]

Ocorre que, com a nova disposição da LGPD, surge a possibilidade que tais dados sejam eliminados à requerimento de seu titular, podendo haver consequências caso a instituição se recuse a fazê-lo.

Se violados os direitos do titular pela empresa, ou qualquer outra previsão da LGPD, caberá denúncia à ANPD (Autoridade Nacional de Proteção de Dados, órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados), que poderá culminar em auditoria e sanções, como a multa e advertência, de acordo com o art. 52 da lei.

A LGPD prevê em seu texto mecanismos protetivos análogos aos previstos no CDC, como a inversão do ônus da prova, o que realça a comunicação entre as fontes.

6 RELATIVIZAÇÃO DO DIREITO À INFORMAÇÃO EM FUNÇÃO DO DIREITO AO ESQUECIMENTO

Aqueles que se posicionam de maneira contrária ao direito ao esquecimento trazem consigo diversas teses argumentativas, como a fragilização da liberdade de expressão, a débil efetividade da medida, a arquitetura da rede, etc.

No entanto, a arguição de que o direito ao esquecimento conflitua com o direito à informação é a de maior relevância para a discussão deste estudo, posto que o cadastro de negativação visa informações pontuais, não assuntos subjetivos.

O direito à informação é indispensável para o Estado Democrático de Direito, marcando diversas relações jurídicas. Para celebrar-se um negócio jurídico com alguém, as partes devem ter plena ciência de quem é a parte contrária. É essencial para qualquer relação jurídica a transparência.

[7]BESSA, Leonardo Roscoe. Código de Defesa do Consumidor comentado. Rio de Janeiro: Forense, 2020. Livro Digital. (1 recurso online). ISBN 9788530992132.

Se determinado indivíduo deseja celebrar um empréstimo consignado com uma instituição bancária, deve ter acesso aos seus precedentes financeiros, por exemplo.

É irrefutável a necessidade de fornecimento de dados sobre quem é a pessoa do consumidor. Não obstante, há um limite imposto por norma jurídica que limita o período de tempo no qual pode haver a análise destes dados.

Não obstante, não há, no ordenamento jurídico brasileiro, dentre os direitos e as garantias fundamentais, um que se mostre absoluto e impassível de relativização. É o que ocorre no embate entre o direito ao esquecimento, reflexo ao direito à privacidade, e o direito à informação.

Há hipóteses que, considerada a natureza da relação jurídica, a parte vulnerável precisa de uma proteção para além daquela disposta como regra geral. A dinâmica existente entre o consumidor e as grandes empresas é exemplo de tal fenômeno[8].

7 O "SCORE" COMO PRÁTICA MANIFESTAMENTE ABUSIVA

É fato incontestável que os bancos de dados e cadastros relativos a consumidores, bem como os serviços de proteção ao crédito e aos congêneres são entidades de caráter público, nos termos do art. 43, § 4º, CDC.

Analisando-se as decisões pátrias acerca da inserção de débitos prescritos nas plataformas destas entidades, há o "Serasa Limpa Nome", plataforma na qual estão cadastradas dívidas prescritas para a cobrança judicial (art. 206, § 5º, I, CC), mas que persistem enquanto obrigação natural.

Em diversos julgados, o SERASA "Serasa Limpa Nome" sustenta que terceiros não têm acesso às informações registradas nos bancos de dados dos serviços de proteção ao crédito dispostos na plataforma "Serasa Limpa Nome". Não obstante, tal afirmação não merece guarida, considerando-se o disposto nos Termos de Uso e Políticas de Privacidade da Serasa, disponível no sítio eletrônico do órgão. Observe-se:

> "5. A quem a Serasa Experian disponibiliza os dados coletados?
> A Serasa Experian trata apenas os Dados que entende serem os mínimos necessários para cada finalidade e, em razão disso, poderá disponibilizar seus Dados apenas para as pessoas e empresas que consultam os serviços da Serasa Experian para as finalidades descritas no item 3, acima.
> A Serasa Experian também **pode disponibilizar os Dados, quando estritamente necessário, a (i) empresas do grupo Experian que gerenciam algumas partes dos serviços, (ii) fornecedores e (iii) revendedores, distribuidores e agentes envolvidos na prestação dos serviços.**" (grifos nossos)

[8]REIS, Sergio Cabral dos. Tutela processual dos direitos: a superação da irreversibilidade fática dos efeitos da tutela antecipada. Ciência Jurídica do Trabalho, Belo Horizonte, MG, v. 15, n. 93, p. 09-32, maio/jun. 2012.

Reputa-se configurada, nesse diapasão, a possibilidade de disponibilização a terceiros, podendo haver influência de forma negativa.

Nesse sentido, já decidiu o Egrégio Tribunal de Justiça de São Paulo, *in verbis*:

> "Apelações – Ação declaratória c.c. indenizatória – Débito prescrito apontado no "Serasa Limpa Nome" - Sentença de acolhimento do pedido declaratório e de rejeição do indenizatório. 1. Débito prescrito, o que não se discute. Declaração da inexigibilidade da dívida que se impõe, em virtude da extinção do direito de reclamá-la em juízo, mercê da prescrição. 2. Pedido cominatório de abstenção dos atos de cobrança que se acolhe, pois não se justifica reconhecer ao credor o direito de realizar cobranças extrajudiciais, sobretudo no âmbito de relações de consumo, sob pena de fazer indefinida a questão e deixar o consumidor, permanentemente, sujeito a importunações. 3. Consequente determinação para cancelamento daquela anotação, inclusive para que não reflitam na formação do chamado "score". Do contrário, estaríamos admitindo que nosso sistema jurídico contempla sanção eterna, já que o devedor, em tal hipótese, jamais se livraria da pecha de mau pagador ou, o que dá na mesma, das respectivas consequências, pese a prescrição. 4. Não demonstrado, porém, o efetivo caráter restritivo do cadastro em questão, isto é, a possibilidade de trazer algum tipo de comprometimento à imagem da autora no meio social, em termos de abalo ao crédito. Dano moral não caracterizado. Precedentes desta Corte. 5. Sentença reformada, para acolhimento do pedido voltado ao cancelamento da anotação e do cominatório. Responsabilidades pelas verbas da sucumbência distribuídas em proporção. Deram parcial provimento a ambas as apelações." (TJSP; Apelação Cível 1009516-42.2020.8.26.0223; Relator (a): Ricardo Pessoa de Mello Belli; Órgão Julgador: 19ª Câmara de Direito Privado; Foro de Guarujá - 3ª Vara Cível; Data do Julgamento: 08/11/2021; Data de Registro: 10/11/2021)
>
> "APELAÇÃO – Ação de obrigação de fazer c.c indenização por danos morais. Indenização por dano moral afastada por não haver negativação da dívida, mas apenas constar no Serasa "limpa nome" como "contas atrasadas", verificada apenas mediante acesso exclusivo do consumidor, inexistindo divulgação ou publicação das informações à terceiros. Sentença confirmada por seus próprios fundamentos, nos termos do art. 252 do RITJSP. Cabimento de exclusão da dívida do referido cadastro, já que prescrita, sem interesse de pagamento e sem prejuízo para o credor, que pode cobrá-la extrajudicialmente nos termos do art. 42, "caput", do Código de Defesa do Consumidor. Recurso parcialmente provido" (TJSP; Apelação Cível 1000376-97.2021.8.26.0077; Relator (a): Flávio Cunha da Silva; Órgão Julgador: 38ª Câmara de Direito Privado; Foro de Birigui - 3ª Vara Cível; Data do Julgamento: 17/08/2021; Data de Registro: 17/08/2021)
>
> "AÇÃO DECLARATÓRIA DE INEXIGIBILIDADE DE DÉBITO CUMULADA COM INDENIZAÇÃO POR DANOS MORAIS – Recurso da Ré - Débito decorrente de contrato bancário inscrito na plataforma "serasa limpa nome" - Prescrição reconhecida - Dívida declarada inexigível, determinando-se a abstenção de qualquer ato de cobrança e impondo a condenação por danos morais – Insurgência, objetivando afastar a indenização por danos morais e obter o reconhecimento da exigibilidade da dívida prescrita no âmbito extrajudicial – Acolhimento, em parte - A prescrição extingue o direito do credor à pretensão ao cumprimento da obrigação, mas não implica em extinção da dívida – É possível a mera cobrança extrajudicial, de forma que não implique na publicidade da dívida e não seja abusiva, procedendo-se do modo mais restrito possível, ônus decorrente da perda da pretensão pela inércia - Sistema "serasa limpa nome" que, muito embora seja destinado à composição amigável entre credores e devedores, implica em divulgação de informes desabonadores - Danos morais configurados – Arbitramento da indenização em R$8.000,00 – Pleito de redução – Descabimento - Acolhimento, em parte, do recurso (para ressalvar a possibilidade de cobrança extrajudicial), que aproveita ao corréu que não recorreu (CPC, art. 1.005) - Recurso da Ré provido, em parte. AÇÃO DECLARATÓRIA DE INEXIGIBILIDADE DE DÉBITO CUMULADA COM INDENIZAÇÃO POR DANOS MORAIS – Recurso do Autor – Dívida prescrita

> incluída no sistema "serasa limpa nome" - Danos morais configurados – Arbitramento da indenização em R$8.000,00 – Pleito de majoração – Descabimento – Valor compatível com o quadro fático, tendo em vista o histórico de negativações do nome do Autor e que, embora prescrita, a dívida é existente – Honorários advocatícios arbitrados em 17% do valor da condenação – Pretensão de elevação para 20% do valor da causa – Acolhimento, em parte – Percentual majorado para 20% sobre o valor da condenação - Recurso provido, em parte." (TJSP; Apelação Cível 1000430-71.2020.8.26.0506; Relator (a): Mario de Oliveira; Órgão Julgador: 38ª Câmara de Direito Privado; Foro de Ribeirão Preto - 9ª Vara Cível; Data do Julgamento: 10/08/2021; Data de Registro: 11/08/2021)

Ainda que este não seja o entendimento majoritário, forma-se uma nova linha de enfrentamento da questão, considerados os avanços legislativos e a concretização efetiva dos direitos do consumidor.

8 CONCLUSÃO

À vista do exposto, reputa-se configurada a função da LGPD no que tange o direito ao esquecimento, especialmente no que tange o direito do consumidor.

Não se trata de anistia a todo e qualquer débito, pois o que se busca não é incentivar o inadimplemento, mas sim a persecução do crédito por intermédio de vias que não venham a lesar a honra do consumidor, tal como a própria cobrança judicial.

Nesse diapasão, ainda que seja um tópico relativamente novo no ordenamento jurídico brasileiro, já é palpável a tendência jurisprudencial para que haja a proliferação de um entendimento que venha a proteger o consumidor de forma mais eficaz.

REFERÊNCIAS BIBLIOGRÁFICAS

AZEVEDO, Antonio Junqueira de. A caracterização jurídica da dignidade da pessoa humana. **Revista Trimestral de Direito Civil (RTDC)**. Rio de Janeiro: Padma, 2000. v.1.

CACHAPUZ, Maria Cláudia. Informática e proteção de dados. Os freios necessários à automação. **Revista da Ajuris**, ano XXIV, vol. 70, jul. 1997.

COMENTÁRIOS à Lei Geral de Proteção de Dados. São Paulo: Grupo Almedina, 2020. Livro Digital. (1 recurso online). ISBN 9788584935796.

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

FRAJHOF, Isabella Z. **O direito ao esquecimento na Internet: conceito, aplicação e controvérsias.** São Paulo: Grupo Almedina, 2019. Livro Digital. (1 recurso online). ISBN 9788584934447.

HERMAN, Benjamin. **Código brasileiro de defesa do consumidor**. 10. ed. rev. atual. e reform. Rio de Janeiro: Ed. Forense, 2011. v. I.

PERLINGIERI, Pietro. **Perfis do direito civil. Introdução ao Direito Civil Constitucional.** Rio de Janeiro: Renovar, 1997.

RAMOS FILHO, Evilásio Almeida. **Direito ao esquecimento versus liberdade de informação e de expressão:** a tutela de um direito constitucional da personalidade em face da sociedade de informação.

REIS, Sergio Cabral dos. Tutela processual dos direitos: a superação da irreversibilidade fática dos efeitos da tutela antecipada. **Ciência Jurídica do Trabalho**, Belo Horizonte, MG, v. 15, n. 93, p. 09-32, maio/jun. 2012.

RIFKIN, Jeremy. **A Terceira Revolução Industrial**. Como o poder lateral está transformando a energia, a economia e o mundo. São Paulo: M. Books do Brasil, 2012.

SILVA NETO, Orlando Celso da. **Comentários ao Código de Defesa do Consumidor**. Rio de Janeiro: Forense, 2013. Livro Digital. (1 recurso online). ISBN 978-85-309-5039-2.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. C-131/12. Google Spain SL e Google Inc. vs. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González, j. em 13.05.2014.

LEI DA ANISTIA E O DEVER DE MEMÓRIA

AMNESTY LAW AND THE DUTY TO REMEMBER

JANINE EVANGELISTA[1]

SUMÁRIO: 1. INTRODUÇÃO. 2. ANISTIA. 2.1 Contexto histórico da Lei da Anistia e ADPF nº153. 2.2 Lei da Anistia brasileira e outros casos latino-americanos. 3. DIREITO À MEMÓRIA E À VERDADE. 4. MEMÓRIA NACIONAL E O DIREITO AO ESQUECIMENTO. 4.1 Anistia maior e anistia menor. 4.2 Esquecimento recalque e Esquecimento falsário. 5. CONCLUSÃO. REFERÊNCIA BIBLIOGRÁFICAS.

RESUMO

O presente trabalho tem como principal objetivo tratar sobre a relação estabelecida entre o Direito ao Esquecimento e a Lei da Anistia. Com isso, surge o debate sobre a importância do Direito para a conservação da memória nacional e o poder institucionalizado a esta. Também, é possível analisar o impacto que a decisão do Supremo Tribunal Federal gerou e os efeitos destas na comunidade pública.

Palavras-chave: Direito; Direito ao esquecimento; Lei da anistia; Dever de memória.

ABSTRACT

The present work has as main objective to deal with the relationship established between the Right to Oblivion and the Amnesty Law. With that, the debate arises about the importance of Law for the conservation of national memory and the institutionalized power to it. It is also possible to analyze the impact that the Supreme Court decision generated and the effects of these on the public community.

Keywords: Right. Right to Oblivion; Amnesty Law; Duty of Memory.

1 INTRODUÇÃO

Neste estudo, aborda-se como tema central a relação entre o Direito ao Esquecimento e a Lei da Anistia, vigente em nosso ordenamento jurídico. O Direito ao Esquecimento diz respeito à capacidade que um indivíduo possui de resguardar sua dignidade exigindo que não ocorra divulgação sobre assuntos que versem sobre direitos personalíssimos, poder concedido pela Constituição Federal de 1988: "Artigo 5º, X: São invioláveis a intimidade, a vida privada, a honra e a

[1]Estudante do 4º ano diurno do Curso de Graduação em Direito na Faculdade de Direito de Sorocaba.

imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".[2]

A aplicação desse direito deve trazer benefícios a todos, logo é necessária uma análise concreta sobre o fato, visto que a memória e o interesse público prevalecem diante de situações que solicitam o esquecimento.

A Lei da Anistia é normalmente utilizada em períodos de instabilidade social, política ou em momentos finais de um ciclo, que envolvem algum conflito significante. No Brasil, foi instituída pelo então presidente João Figueiredo, 15 anos após o início do Regime Militar. Tal gradualismo político caracterizou a transição como de tipo pactuada, denominada assim, quando o próprio governo no poder~~,~~ desencadeia o processo de mudança, negociando com a oposição, com o objetivo de manutenção do poder e da autopreservação.

Logo, o assunto abordado gera a discussão se existe relação entre o Direito ao Esquecimento e a Lei da Anistia, e, em caso positivo, se a existência de tal lei não afetaria o direito à Memória Nacional.

2 ANISTIA

A Anistia significa o esquecimento de infrações penais pontuais, logo se exclui o crime e em consequência desaparecem seus efeitos penais.[3] Aplica-se normalmente a crimes políticos em que o Poder Público tem dificuldade em lidar com o ocorrido.

De acordo com a Lei 8.072 de 1990, que disciplina sobre os crimes hediondos em seu artigo 2º inciso I, a anistia é inaplicável aos delitos que se caracterizam pela prática de tortura, tráfico ilícito de entorpecentes e drogas, e o terrorismo.[4]

O indulto concedido tem como principal efeito a extinção da punibilidade penal, porém os efeitos civis podem permanecer a depender do contexto, podendo o acusado inclusive ser condenado ao pagamento dos danos causados à vítima.

De acordo com o autor Júlio Mirabete, existem oito espécies de anistias, são elas:

> 1. Especial: para crimes políticos; 2. Comum: para crimes não políticos; 3. Própria: antes do trânsito em julgado; 4. Imprópria: após o trânsito em julgado; 5. Geral ou plena: menciona apenas os fatos, atingindo todos que a cometeram; 6. Parcial ou restrita: menciona os fatos, mas exige a presença de algum requisito; 7. Incondicionada: não exige a prática de nenhum ato como condição; 8. Condicionada:

[2]BRASIL, Constituição da República Federativa do Brasil (1988). Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 11 ago. 2020.
[3]DELMANTO, Roberto. *Em Defesa do Indulto de Natal*, 2018. Disponível em: https://www.migalhas.com.br/depeso/272077/em-defesa-do-indulto-de-natal. Acesso em: 15 nov. 2020.
[4]BRASIL, Lei dos Crimes Hediondos, 1998. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8072.htm. Acesso em: 15 nov. 2020.

exige a prática de algum ato como condição.[5]

Como dito anteriormente, a anistia exclui todos os efeitos penais decorrentes da infração praticada, porém o benefício refere-se a fatos e não a pessoas envolvidas, podendo ser concedida antes ou após o trânsito em julgado da sentença condenatória, extinguindo o processo de conhecimento ou a sua execução conforme o caso. Se a existência da anistia ocorrer após o trânsito, será denominada como imprópria, e caso ocorra antes, denomina-se como própria.[6]

Em regra, o benefício é incondicionado, ou seja, não há necessidade da prática de nenhum ato como condição, e como consequência não poderá ser recusada pelo beneficiário. Portanto, a Anistia caracteriza pelo seu efeito *ex tunc*, logo apresenta-se com seu efeito retroativo, pois extingue a pretensão punitiva no âmbito criminal, existindo apenas seus efeitos na esfera cível, subsistindo a reivindicação indenizatória.

2.1 Contexto histórico da Lei da Anistia e ADPF nº153

A Lei 6.683 de 1979, denominada Lei da Anistia, foi sancionada em 1979, durante o momento da decadência do regime militar, quando já existia a possibilidade para a volta da democracia. Na época, ocorreram inúmeros protestos, tendo em vista que a comunidade pedia por uma anistia que abrangesse somente os militantes presos ou exilados, porém houve discordâncias sobre o quanto a anistia deveria abranger. Inicialmente, a proposta do governo sugere que os torturadores e membros dos órgãos de repressão seriam anistiados pelos crimes conexos, justamente aqueles que se encadeiam em suas próprias causas, ou seja, são delitos que dependem de outros, devendo sempre existir o nexo de causalidade entre tais, enquanto a contraproposta apresentada pelo Movimento Democrático Brasileiro rejeitava a anistia ampla, defendendo que o ideal seria apenas para os afetados pela ditadura militar.

Finalmente, a proposta do Movimento Democrático foi rejeitada, e a anistia ampla e geral aprovada. Em 2008, a referida lei voltou a ser amplamente discutida visto a condenação do coronel Carlos Alberto Brilhante Ustra. Tão logo, o Conselho Federal da Ordem dos Advogados do Brasil (OAB) propôs, em face do Supremo Tribunal Federal, uma Arguição de Preceito Fundamental, a ADPF nº 153, com o intuito de obter do STF uma análise da Lei da Anistia conforme a Constituição Federal, retirando a proteção dos crimes políticos dos agentes da repressão que atuaram por 21 anos.

[5] MIRABETE, Julio Fabbrini. *Execução Penal.* 11ª ed. Atlas: São Paulo, 2004, p. 781.
[6]BRITO, Alexis Augusto Couto de. *Execução Penal*. 4ª ed. Editora Saraiva, 2018. p. 365.

A ADPF nº 153 foi julgada improcedente pelo Supremo Tribunal Federal, em abril de 2010, por sete votos contra dois. O então presidente do STF, ministro Cezar Peluso, justificou seu voto contrário, dizendo que "Só o homem perdoa, só uma sociedade superior qualificada pela consciência dos mais elevados sentimentos de humanidade é capaz de perdoar. Porque só uma sociedade que, por ter grandeza, é maior do que o seu inimigo, é capaz de sobreviver." [7]

Os 2 (dois) ministros que votaram a favor de uma revisão foram os ministros Ricardo Lewandowski e Ayres Britto. Em seus pareceres, eles afirmam que certos crimes são incompatíveis com a criminalidade por conexão.

Os juristas que defendem a anistia a todos os envolvidos embasam a argumentação no Princípio da Irretroatividade da Lei Penal mais severa, que estabelece a irretroatividade da lei penal, salvo em benefício ao réu. Logo, uma lei posterior não pode atingir os beneficiados pela anistia diante do caráter prejudicial aos réus. Aplica-se, dessa forma, essa decisão tanto aos membros do governo, quanto aos militantes, mas há a exceção dos crimes de caráter permanentes e continuados, como é o caso dos desaparecidos políticos, que, de acordo com a Comissão Nacional da Verdade (CNV), são 210 pessoas.

Na contramão, há aqueles que argumentam que a Constituição Federal de 1988 tornou o crime de tortura inafiançável e, diante da gravidade, escapa-se o benefício da anistia. Somado a isto, existe também a pressão internacional referente ao esforço do Estado em reparar e punir as violações de direitos humanos ocorridos em nossa jurisdição.

2.2 Lei da Anistia brasileira e outros casos latino-americanos

O esforço do Estado brasileiro, em punir as torturas cometidas na ditadura militar, mostra-se muito pequeno em comparação a outros países latino-americanos. No Chile, a ditadura militar teve fim em 1990, e como no Brasil foi instituída a Lei da Anistia, que protege os militares dos crimes cometidos entre setembro de 1973 e abril de 1978, a situação é diferente (sugestão). A Comissão Nacional de Prisão Política e Tortura estima que entre 1973 e 1990, 3225 pessoas foram mortas ou estão desaparecidas.

Dois casos específicos abriram precedentes para a condenação de outros militares pós-ditadura, que praticaram condutas semelhantes: o caso do estudante Juan Cheuquepán e do agricultor José Julio Llaulén Antilao, que após serem presos nunca mais foram vistos,

[7]BRASIL, Supremo Tribunal Federal. Arguição de Descumprimento de Preceito 153 Distrito Federal, 2010. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=612960> Acesso em: 05 mar. 2020.

configurando um delito permanente, pois ambos continuam desaparecidos.

Em 1998, a Suprema Corte decidiu que a Lei da Anistia não poderia ser utilizada em casos de violações dos direitos humanos, a medida permitiu que uma série de investigações tivessem início, condenando cerca de 250 pessoas acusadas de assassinato e tortura. A justiça chilena enquadrou os crimes praticados pelo Estado como crimes contra a humanidade.

Outro caso curioso refere-se ao período ditatorial na Argentina. A ditadura argentina ocorreu entre 1966 e 1973, depois novamente entre 1976 e 1983. Ao fim da ditadura, também foi instaurada a Lei da Anistia, marcando o processo de transição.

O presidente eleito, Raúl Alfonsín, deu início ao projeto de lei intitulado Lei do Ponto Final, que determinava uma data limite para o julgamento dos envolvidos, e a Lei da Obediência Civil, que estabelecia a impunidade aos oficiais de média patente, visto que tais militares estariam cumprindo ordens superiores.

A Argentina foi o primeiro país na América Latina a julgar militares envolvidos nas violações dos direitos humanos. Em 2005, as leis referentes ao período militar foram oficialmente anuladas, com o argumento de que a manutenção destas normas violava a Constituição e, com esse fim, iniciou-se novamente a retomada de instauração de processos. Estima-se que 200 militares foram condenados pelos crimes praticados durante o período ditatorial.

3 DIREITO À MEMÓRIA E À VERDADE

O 3º Programa Nacional de Direitos Humanos (PNDH) estabeleceu um roteiro com a finalidade de guiar o Estado brasileiro na busca pelo monitoramento de políticas públicas voltadas aos direitos humanos.

O Programa tratou a ditadura militar como uma política de memória para os crimes praticados nesse período, estabelecendo três diretrizes políticas que o país deveria adotar para consolidar o dever de memória sobre esse período, a saber:

> Diretriz 23: Reconhecimento da memória e da verdade como Direito Humano da cidadania e dever do Estado; Diretriz 24: Preservação da memória histórica e a construção pública da verdade; Diretriz 25: Modernização da legislação relacionada com a promoção do direito à memória e à verdade, fortalecendo a democracia.[8]

O PNDH-3 define o direito à memória como:

> O trabalho de reconstituir a memória exige revisitar o passado e compartilhar experiências de dor, violência e mortes. Somente depois de 204embra-las e fazer seu

[8]BRASIL, Terceiro Programa Nacional de Direitos Humanos, 2009. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/decreto/d7037.htm. Acesso em: 05 jul. 2020.

> luto, será possível superar o trauma histórico e seguir adiante. A vivência do sofrimento e das perdas não pode ser reduzida a conflito privado e subjetivo, uma vez que se inscreveu em um contexto social, e não individual.[9]

Fabiana Dantas destaca que o exercício do direito de memória pode ser compreendido em dois aspectos, são eles:

> O primeiro, de aprendizagem das experiências sociais passadas, que servem de orientação e base para a construção de um futuro melhor; e, em segundo lugar, a formação da consciência de pertença do indivíduo ao grupo (identidade cultural) fundamental para sua inserção política e para o exercício efetivo de sua cidadania.[10]

Para isso, como bem afirma a autora, o direito à memória também exige a reconstrução crítica dos aspectos do passado, ocorrendo com o intuito de viabilizar o crescimento social (elaboração).

4 MEMÓRIA NACIONAL E O DIREITO AO ESQUECIMENTO

O autor e professor Sérgio Branco une características para decifrar o que é ou não o Direito ao Esquecimento. Segundo o docente, não será objeto do esquecimento os assuntos que envolverem interesses públicos e eventos históricos que afetam a memória nacional.[11]

Para Celso Antônio Bandeira de Mello, o interesse público qualifica-se como interesse resultante do conjunto dos interesses que os indivíduos pessoalmente têm quando considerados em sua qualidade de membros da Sociedade e pelo simples fato de o serem.[12] Logo, deve ser levado em conta o interesse da sociedade, mas também o interesse particular de um indivíduo que se insere na coletividade.

Também, é critério de análise os eventos históricos e o Dever de Memória decorrente destes. Neste caso, há uma modificação da sociedade vigente, tendo em vista que um fato social altera todo o plano sequência, sendo necessário para a compreensão do presente o entendimento do fato que ocorreu no passado. A ignorância sobre o ocorrido pode gerar problemas no presente diretamente ligados ao esquecimento do fato de importância social.

O jurista belga François Ost escreve sobre o importante papel do Direito na memória nacional: "A coletividade só é construída com base numa memória compartilhada, e é ao

[9]BRASIL, Terceiro Programa Nacional de Direitos Humanos, 2009. Disponível em: http://www.dhnet.org.br/pndh/6memoria/index.htm> Acesso em: 05 jul. 2020.
[10]DANTAS, Fabiana Santos. Direitos; Memória individual e coletiva; Patrimônio cultural, 2008. p. 19 Disponível em: https://repositorio.ufpe.br/bitstream/123456789/4176/1/arquivo6343_1.pdf. Acesso em 06 jul. 2020.
[11]BRANCO, Sérgio. Memória e Esquecimento na Internet. Porto Alegre: Arquipélago Editorial, 2017. p. 172/176.
[12]MELLO, Celso Antônio Bandeira de. Curso de Direito Administrativo. 26. ed. São Paulo: Malheiros, 2009. p. 61.

Direito que cabe instituí-la"[13]. Nota-se, nesse trecho, a importância do Direito que carrega o fardo de resguardar a memória e definir inclusive as próximas gerações.

Desde as eleições presidenciais de 2018, vem ocorrendo o avanço das discussões referentes à volta de uma possível ditadura militar, acalentadas com o pretexto de um regime salvador que colocaria o país nos eixos após uma crise social, política e econômica. Resta a dúvida se a Lei da Anistia influenciou tal movimento.

William Faulkner, em seu romance publicado em 1950, escreve que "O passado nunca está morto. Nem sequer passou"[14]. (coesão) O assunto continua atual como já o foi há 35 anos, visto que o fato histórico é de extrema importância e deveria ser debatido nos ambientes adequados, para que a sociedade compreenda o que é uma ditadura e como ela se contrapõe ao regime democrático. Como o assunto (palavra excessivamente genérica) foi encoberto, criou-se um mito em torno do tema, que não deixou de ser discutido, porém foi feito sem base histórica e sem senso crítico, não sendo estudado e ensinado por profissionais qualificados, tornando-se, assim, um assunto reconhecido por toda comunidade, mas sem embasamento crítico.

De fato, certos aspectos passaram a ser essenciais para a população contemporânea após as grandes guerras mundiais, são eles: o direito à memória, à verdade, à reparação, à justiça e ao fortalecimento das instituições democráticas.

4.1 Anistia maior e anistia menor

O jurista François Ost desenvolveu uma classificação para identificar anistias, caracterizadas por ele como anistia maior e menor.

A anistia "menor" apresenta uma efetiva possibilidade de perdão, pois ocorrerá um processo contra os acusados. Só existe perdão quando houver um procedimento que discuta as práticas criminosas. Neste caso, admite-se o ocorrido e há a efetiva possibilidade de condenação ou perdão pelo benefício da anistia.

Já na anistia "maior", extingue-se a possibilidade de existir ação penal, pois os fatos são modificados e os crimes descritos nos tipos penais incriminadores deixam de existir com a argumentação embasada no contexto social vivido, impondo que tais crimes foram socialmente necessários para conter outros crimes, ou seja, crimes conexos.

A Lei 6.683, de 1979, apresenta-se como uma anistia "maior", dado que após o fim da

[13] OST, François. O Tempo do Direito. São Paulo: Instituto Piaget, 2001. p. 47.
[14]FAULKNER, William. Réquiem para uma freira. Lisboa: Fólio, 1958. p. 107.

ditadura militar comportam-se como se os crimes não tivessem ocorrido. A anistia consiste, como já foi dito, no ato de perdoar, porém a existência desta não implica o esquecimento sobre o ocorrido, ou seja, o ato deveria ter sido reconhecido e estudado.

4.2 Esquecimento recalque e Esquecimento falsário

De acordo com Ost, há categorias de esquecimento, sendo elas o Esquecimento recalque e o Esquecimento falsário.

O Esquecimento recalque mostra uma história contada por vencedores, visando apagar as situações impostas às pessoas que foram contrárias ao movimento. É o esquecimento que ocorreu no Brasil, pois, durante o próprio regime militar, a Lei da Anistia foi criada e elaborada pelos próprios militares, ou seja, os fatos foram narrados e determinados por estes.

Já no Esquecimento falsário, os vencedores apresentam inúmeras mentiras para legitimar o ato, ou seja, reconhecem o ato, porém de uma maneira deturpada.

A Lei da Anistia é considerada por muitos uma lei "dupla via", como um benefício recíproco, já que foram também anistiadas as pessoas contrárias ao regime, como os agentes do Estado que praticaram os crimes políticos e conexos. Assim, criou-se a ilusão que a sociedade estava retornando ao normal, e os direitos sendo restabelecidos. Porém, resistiu para os familiares dos mortos, desaparecidos e torturados o sentimento de impunidade, de uma justiça falha que anistiou os agentes da repressão sem instaurar processos para averiguar os casos.

Vemos que a classificação de Ost encaixa-se no Brasil, já que a Lei da Anistia é maior e nosso esquecimento é o recalque.

5 CONCLUSÃO

Como foi analisado, a Lei da Anistia referente ao Regime Militar brasileiro enquadra-se como uma concessão do Direito ao Esquecimento que privilegiou os agentes do Estado. Certamente, como foi citado anteriormente, o direito oferecido fere as características essenciais dos casos em que o esquecimento pode ser oferecido, pois possui as características presentes em um fato histórico de relevante interesse público. Tal interesse é comprovado pela polarização que se observa atualmente pelos grupos contrários e favoráveis a um possível retorno do Regime Militar.

A Anistia caracteriza-se pelo perdão e adentra o Direito ao Esquecimento. O Estado Democrático tem o dever de memória, tendo o poder de prevenir que a história se repita

novamente, podendo reparar os danos de quem sofreu no passado. Não pode haver o perdão se não se conhece aquilo que foi perdoado.

Como um aspecto da justiça de transição, que normalmente ocorre após um regime autoritário, temos o Direito à verdade e à memória. Um motivo claro pela busca desse direito é a necessidade que os fatos fiquem claros para todos que não vivenciaram o ocorrido nitidamente, com o intuito que a circunstância não se repita.

Para o fortalecimento das instituições democráticas, é necessário a investigação dos crimes praticados durante uma ditadura, especificando a responsabilidade de cada agente.

De fato, a Lei da Anistia brasileira mostra como a justiça de transição foi falha ao não assegurar o Direito à memória e o direito à verdade, contribuindo para uma série de problemas em nossa democracia. Avançamos com a instituição da Comissão Nacional da Verdade, porém a responsabilização dos agentes ainda é falha e, no limite, inexistente. A impunidade reflete-se na continuidade da violência das forças de segurança do país, que ainda consideram os métodos de tortura viáveis em uma sociedade democrática.

Portanto, o governo autoritário utilizou-se do Direito ao Esquecimento como uma forma de blindar-se de futuras investigações sobre os atos atentatórios aos direitos humanos ocorridos no período ditatorial, afetando inevitavelmente o Direito à memória nacional. Dantas (2008) argumenta que "o direito fundamental à memória corresponde à necessidade individual e coletiva de afirmação e conhecimento atuais do passado"[15]. Como não nos foi dada a oportunidade de tomar conhecimento sobre o que ocorreu, resta dizer que o princípio inerente à memória social foi violado.

REFERÊNCIA BIBLIOGRÁFICAS

BRANCO, Sérgio. **Memória e esquecimento na internet.** Porto Alegre: Arquipélago Editorial, 2017.

BRASIL, **Constituição da República Federativa do Brasil (1988).** Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 02 jul. 2020.

BRASIL, **Lei dos Crimes Hediondos, 1998.** Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8072.htm. Acesso em: 15 nov. 2020.

[15]DANTAS, Fabiana Santos. Direitos; Memória individual e coletiva; Patrimônio cultural, 2008. p. 08. Disponível em: https://repositorio.ufpe.br/bitstream/123456789/4176/1/arquivo6343_1.pdf. Acesso em 06 jul. 2020.

BRASIL, Supremo Tribunal Federal. **Arguição de Descumprimento de Preceito 153 Distrito Federal,** 2010. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=612960. Acesso em: 05 mar. 2020.

BRASIL, **Terceiro Programa Nacional de Direitos Humanos, 2009.** Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/decreto/d7037.htm. Acesso em: 05 de jul. 2020.

BRASIL, **Terceiro Programa Nacional de Direitos Humanos, 2009**. **Dhnet.** Disponível em: http://www.dhnet.org.br/pndh/6memoria/index.htm. Acesso em: 05 de jul. 2020.

BRASIL. **Lei da Anistia. Lei nº 6683, de 28 de agosto de 1979.** Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L6683.htm. Acesso em: 14 maio 2020.

BRITO, Alexis Augusto Couto de. **Execução Penal,** 4. ed. Editora Saraiva, 2018. p. 365.

DANTAS, Fabiana Santos. Direito fundamental à Memória, Patrimônio cultural, 2008. p. 19. **Repositório Institucional da Universidade Federal de Pernambuco (UFPE)**. Disponível em: https://repositorio.ufpe.br/bitstream/123456789/4176/1/arquivo6343_1.pdf. Acesso em 06 jul. 2020.

DELMANTO, Roberto. **Em Defesa do Indulto de Natal,** 2018**. Migalhas.** Disponível em: https://www.migalhas.com.br/depeso/272077/em-defesa-do-indulto-de-natal. Acesso em: 15 nov. 2020.

GUMIERI, Julia Cerqueira. **A Construção Possível: inclusão e revisão do direito à memória e à verdade no 3° Programa Nacional de Direitos Humanos.** 2016. Dissertação (Mestrado em História Social) - Faculdade de Filosofia, Letras e Ciências Humanas,

LENZA, Pedro. **Direito Constitucional Esquematizado.** 23. ed. São Paulo: Saraiva Educação, 2019.

MASSON, Cleber. **Direito Penal - Parte Geral.** São Paulo: Grupo Gen, 2018.

MILHORANZA, Mariângela Guerreiro. O Tempo do Direito**,** 2008. **UFPEL**. Disponível em: https://www.paginasdedireito.com.br/index.php/artigos/66-artigos-abr-2008/6062-resenha-do-livro-o-tempo-do-direito-de-autoria-de-francois-ost. Acesso em: 05 ago. 2020.

MIRABETE, Júlio Fabbrini. **Execução Penal.** 11. ed. São Paulo: Atlas, 2004.

MIRABETE, Júlio. **Manual de Direito Penal.** São Paulo: Atlas, 2019.

OST, François. **O Tempo do Direito.** Instituto Piaget, 2001.

OSTJEN, Linda. O Tempo do Direito, 2006. **Migalhas.** Disponível em: https://www.migalhas.com.br/depeso/20276/o-tempo-do-direito. Acesso em: 05 ago. 2020.

REVISTA ANISTIA POLÍTICA E JUSTIÇA DE TRANSIÇÃO. **Memorial da Anistia**. Disponível em: http://memorialanistia.org.br/anistia-e-jutica-de-transicao/. Acesso em: 14 jul. 2020.

SOUZA, Arnaldo Vieira. O Direito Entre a Memória e o Esquecimento, 2014. **UNDB.** Disponível em: http://sou.undb.edu.br/public/publicacoes/4_-_lei_da_anistia.pdf. Acesso e: 14 ago. 2020.

T. Montenegro, Antônio; S. Rodeghero Carla; PAULA, Maria Araújo. **Marcas da Memória:** história oral da anistia no Brasil. Editora Universitária da UFPE, Recife, 2012.

UNIVERSIDADE DE SÃO PAULO. São Paulo, 2017. **USP**. Disponível em: https://teses.usp.br/teses/disponiveis/8/8138/tde-14062017-092258/publico/2016_JuliaCerqueiraGumieri_VOrig.pdf. Acesso em: 14 jul. 2020.