DIGESTO

A Revista Jurídica do ISM – Instituto Silvio Meira

"Temas de Direito Digital e Tecnologia"

5ª Edição

ANDRÉ AUGUSTO MALCHER MEIRA
FLAVIA CHRISTIANE ALCÂNTARA FIGUEIRA
MARINA ANDRADE DA GAMA MALCHER GATO
(Coordenadores)

DIGESTO

A Revista Jurídica do ISM – Instituto Silvio Meira

"Temas de Direito Digital e Tecnologia"

5ª Edição

Em homenagem post mortem a LUIZ PAULO MALCHER

Belo Horizonte
2024

Impresso no Brasil | Printed in Brazil

Arraes Editores Ltda., 2024.

Coordenação Editorial: Fabiana Carvalho
Produção Editorial e Capa: Danilo Jorge da Silva
Revisão: Responsabilidade do Autor

342.1
D572
2024

Digesto: a Revista Jurídica do ISM – Instituto Silvio Meira: temas de direito digital e tecnologia: em homenagem *post mortem* a Luiz Paulo Malcher. 5. ed. / [coordenado por] André Augusto Malcher Meira, Flavia Christiane Alcântara Figueira [e] Maria Andrade da Gama Malcher Gato.
Belo Horizonte: Arraes Editores, 2024.
178 p.

ISBN: 978-65-5929-444-2
ISBN: 978-65-5929-448-0 (E-book)
Vários autores.

1. Direito 2. Direito digital. 3. Direito tecnológico. 4. Direito de família. 5. Agronegócio. 6. Relações comerciais. 7. Relações de consumo. 8. Phishing. 9. Direito processual – Provas digitais. 10. Metaverso – Brasil. 11. Neurofeedback. 12. Inteligência artificial. 13. Segurança cibernética. 14. Redes sociais – Influências. 15. E-notariado. I. Meira, André Augusto Malcher (Coord.). II. Figueira, Flavia Christiane Alcântara (Coord.). III. Gato, Maria Andrade da Gama Malcher (Coord.). IV. Malcher, Luiz Paulo (*in memoriam*). III. Digesto – a Revista Jurídica do ISM. IV. Instituto Silvio Meira – ISM. V. Título.

CDDir – 342.1
CDD (23. ed.) – 342.085

Elaborada por: Fátima Falci
CRB/6-700

Matriz
Av. Nossa Senhora do Carmo, 1650/loja 29 - Bairro Sion
Belo Horizonte/MG - CEP 30330-000
Tel: (31) 3031-2330

Filial
Rua Senador Feijó, 154/cj 64 – Bairro Sé
São Paulo/SP - CEP 01006-000
Tel: (11) 3105-6370

www.arraeseditores.com.br
arraes@arraeseditores.com.br

Belo Horizonte
2024

INSTITUTO SILVIO MEIRA – ACADEMIA DE DIREITO

www.institutosilviomeira.net.br

DIRETORIA

André Augusto Malcher Meira
Presidente

Roberta Menezes Coelho de Souza
Vice-presidente

Bruno Menezes Coelho de Souza
Diretor Secretário

Eduardo Vera-Cruz Pinto
Diretor Geral em Lisboa

Raimundo Chaves Neto
Diretor em Lisboa

Ana Patrícia Lima Freire
Diretora em Lisboa

Maria José Motta Sobreira
Diretora em Lisboa

MEMBROS

MEMBROS BENEMÉRITOS

1. ALUÍSIO AUGUSTO MARTINS MEIRA
2. ANTÔNIO MARIA FILGUEIRAS CAVALCANTE (*in memoriam*)
3. MARIA BETÂNIA FIDALGO ARROYO
4. MARIA HELENA DINIZ
5. MAURO IMBIRIBA CORRÊA
6. RITA DE CÁSSIA SANT ANNA CORTEZ

MEMBROS HONORÁRIOS

1. JÚLIO ANTÔNIO JORGE LOPES
2. VIVIANE COÊLHO DE SÉLLOS-KNOERR
3. MINISTRO JOSÉ BARROSO FILHO
4. INSTITUTO LUDOVICUS - CÂMARA CASCUDO

MEMBROS EFETIVOS

1. ADHERBAL MEIRA MATTOS
2. ADRIANA MALCHER MEIRA ROCHA
3. ANA MARIA BARATA
4. ANA CAROLINA BETZEL
5. ANDRESSA NERY LAMARÃO
6. ÂNGELA SABÁT
7. ÂNGELA SERRA SALLES
8. ANTÔNIO JOSÉ DE MATTOS NETO
9. AVELINA HESKET
10. BRUNA KOURY
11. BRUNO MENEZES COELHO DE SOUZA
12. CESAR BECHARA NADER MATTAR JR
13. CLODOMIR ARAÚJO JR
14. CLÓVIS CUNHA DA GAMA MALCHER FILHO
15. ELDER LISBOA DA COSTA - (*in memoriam*)
16. ERNANE MALATO
17. EULINA MAIA
18. EVA FRANCO
19. FABRÍCIO VASCONCELOS DE OLIVEIRA
20. FLÁVIA CHRISTIANE ALCÂNTARA FIGUEIRA
21. FREDERICO ANTÔNIO LIMA DE OLIVEIRA
22. GABRIELA HOLANDA CASTRO
23. HOMERO LAMARÃO NETO
24. JEFERSON ANTÔNIO FERNANDES BACELAR
25. JOSÉ HENRIQUE MOUTA ARAÚJO
26. JUSSARA DERENJI
27. LUCIANA MARIA MALCHER MEIRA
28. LUISA CHAVES
29. MAGDA ABOU EL HOSN
30. MARCELO HOLANDA
31. MARINA ANDRADE DA GAMA MALCHER GATO

32. MARINA PANTOJA BERNARDES
33. MILTON AUGUSTO DE BRITO NOBRE
34. NEY MARANHÃO
35. PASTORA DO SOCORRO TEIXEIRA LEAL
36. PAULA FRASSINETTI MATTOS
37. PAULO DE TARSO DIAS KLAUTAU FILHO
38. PERLLA PEREIRA
39. RAPHAEL SAMPAIO VALE
40. RENAN VIEIRA DA GAMA MALCHER
41. ROBERTA MENEZES COELHO DE SOUZA
42. RUI FRAZÃO DE SOUSA
43. SERGIO ALBERTO FRAZÃO DO COUTO (*in memoriam*)
44. THADEU DE JESUS E SILVA
45. VICTOR AUGUSTO DE OLIVEIRA MEIRA
46. ZENO VELOSO (in memoriam)
47. ZILAH MARIA CALLADO FADUL PETERSEN

SÓCIOS CORRESPONDENTES

1. ANA PATRÍCIA LIMA FEIRE - PERNAMBUCO E LISBOA
2. ANA PAULA BALBINO - MINAS GERAIS
3. AURÉLIO WANDER BASTOS - RIO DE JANEIRO
4. AURINEY BRITO - AMAPÁ
5. AUSTRÉIA MAGALHÃES CÂNDIDO - SÃO PAULO
6. CARMELA GRUNE - RIO GRANDE DO SUL
7. CLÁUDIO HENRIQUE DE CASTRO - PARANÁ
8. EDIT OLIVEIRA - LISBOA
9. EDUARDO SERUR- PERNAMBUCO
10. ELIZA GONÇALVES DIAS - CEARÁ
11. HÉLIO GUSTAVO ALVES - SANTA CATARINA
12. JOSÉ HORÁCIO HALFELD REZENDE RIBEIRO - SÃO PAULO
13. LILIAN AZEVEDO - ROMA
14. MARIANNA CHAVES - PARAÍBA E COIMBRA
15. RAIMUNDO CHAVES NETO - CEARÁ E LISBOA
16. RICARDO BEZERRA - PARAÍBA
17. ROBERTA AVELINE - ROMA / ITÁLIA
18. ROBERTO VICTOR PEREIRA RIBEIRO - CEARÁ
19. RODOLFO PAMPLONA FILHO - BAHIA
20. RODRIGO LIMA VAZ SAMPAIO - SÃO PAULO
21. SOFIA MIRANDA RABELO - MINAS GERAIS
22. VIVIANE SÉLLOS KNOÉRR - PARANÁ

REALIZAÇÕES ISM

- I CONGRESSO LUSO-BRASILEIRO DE DIREITO (SET/2013) – BELÉM
- II CONGRESSO LUSO-BRASILEIRO DE DIREITO (SET/2014) – BELÉM (em homenagem a Egydio Machado Salles)
- III CONGRESSO LUSO-BRASILEIRO DE DIREITO (MAIO/2015) – LISBOA
- IV CONGRESSO LUSO-BRASILEIRO DE DIREITO (SET/2015) – BELÉM (em homenagem a Zeno Veloso)
- V CONGRESSO LUSO-BRASILEIRO DE DIREITO (ABRIL/2016) – LISBOA (em homenagem a Clóvis Malcher)
- XVIII CONGRESSO INTERNACIONAL E XXI CONGRESSO IBEROAMERICANO DE DIREITO ROMANO (AGOSTO/2016) – BELÉM (em homenagem a Clóvis Malcher)
- VI CONGRESSO LUSO-BRASILEIRO DE DIREITO (MAIO/2017) – LISBOA (em homenagem a Daniel Coelho de Souza)
- XXIV FÓRUM DE CIÊNCIA PENAL (SETEMBRO/2017) – FORTALEZA
- VISITA OFICIAL NA OMC – ORGANIZAÇÃO MUNDIAL DO COMÉRCIO (ABRIL/2015) – GENEBRA/SUÍÇA
- I CONGRESSO LUSO-ÍTALO-BRASILEIRO DE DIREITO (23 e 24 de ABRIL de 2018) – VATICANO/ROMA/ITÁLIA (em homenagem a Arnaldo Meira)
- VII CONGRESSO LUSO-BRASILEIRO DE DIREITO (18 e 19 de OUTUBRO de 2018) – LISBOA/PORTUGAL (em homenagem a Adherbal Meira Mattos)
- II CONGRESSO ÍTALO-LUSO-BRASILEIRO DE DIREITO (25 e 26 de MARÇO de 2019) – ROMA/ITÁLIA (em homenagem ao centenário do nascimento do jurista Silvio Meira)
- SIMPÓSIO DE DIREITO ROMANO (14 de MAIO de 2019) – RIO DE JANEIRO (em homenagem ao centenário do nascimento do jurista Silvio Meira)
- COLUNBRADEC – CONGRESSO LUSO-BRASILEIRO DE DIREITO EMPRESARIAL E CIDADANIA (14 de MAIO de 2019) – CURITIBA/PA (em homenagem ao centenário do nascimento do jurista Silvio Meira – em parceria com o UNICURITIBA)
- ENCONTRO LUSO-BRASILEIRO DE DIREITO (27 de SETEMBRO de 2019) – LISBOA/PT (em homenagem ao centenário do nascimento do jurista Silvio Meira)
- VIII CONGRESSO LUSO-BRASILEIRO DE DIREITO (09 e 10 de OUTUBRO de 2019) – BELÉM/PA (em homenagem ao centenário do nascimento do jurista Silvio Meira)
- SIMPÓSIO DE DIREITO AMAZÔNICO (08 de NOVEMBRO de 2019) – BELÉM/PA em homenagem ao centenário do nascimento do jurista Silvio Meira)
- 30 “LIVES” virtuais na época da pandemia Covid-19

- I CONGRESSO FRANCO-BRASILEIRO DE DIREITO (09 e 10 de MARÇO de 2022) – PARIS / FRANÇA (em homenagem aos 50 anos de formado do jurista FREDERICO COELHO DE SOUZA – "in memoriam")
- III CONGRESSO ÍTALO-LUSO-BRASILEIRO DE DIREITO (10 e 11 de OUTUBRO de 2022) – ROMA/ITÁLIA (em homenagem aos 50 anos de formado do jurista FREDERICO COELHO DE SOUZA – "in memoriam")
- IX CONGRESSO LUSO-BRASILEIRO DE DIREITO (13 e 14 de OUTUBRO de 2022) – LISBOA/PT (em homenagem aos 50 anos de formado do jurista FREDERICO COELHO DE SOUZA – "in memoriam")
- X CONGRESSO LUSO-BRASILEIRO DE DIREITO (30 e 31 de MARÇO de 2023) – FUNCHAL/ILHA DA MADEIRA/PORTUGAL (em homenagem aos 10 anos do ISM)
- IV CONGRESSO ÍTALO-LUSO-BRASILEIRO DE DIREITO (02 e 03 de OUTUBRO de 2023) – ROMA/ITÁLIA (em homenagem aos 10 ANOS DO ISM)
- II SIMPÓSIO DE DIREITO AMAZÔNICO (27 de OUTUBRO de 2023 – BELÉM/PA)
- I CONGRESSO BRASIL GERMÂNICO DE DIREITO (29 e 30 de ABRIL de 2024) – FRAKFURT/ALEMANHA
- III SIMPÓSIO DE DIREITO AMAZÔNICO (30 de AGOSTO de 2024 – MANAUS/AM)

PRÓXIMAS REALIZAÇÕES

- V CONGRESSO ÍTALO-LUSO-BRASILEIRO DE DIREITO (23 e 24 de SETEMBRO de 2024) – ROMA/ITÁLIA
- I ISM WTO FORUM SUMMIT DE DIREITO COMERCIAL E COMÉRCIO INTERNACIONAL (22 de NOVEMBRO de 2024) – GENEBRA/SUÍÇA

PRÊMIO SILVIO MEIRA - LISTA DE PREMIADOS

- ANA PATRÍCIA LIMA FREIRE
- CÉSAR BECHARA NADER MATTAR JR
- CLÓVIS CUNHA DA GAMA MALCHER (*in memoriam*)
- CLÓVIS CUNHA DA GAMA MALCHER FILHO
- DES. CÉLIA REGINA DE LIMA PINHEIRO
- DANIEL QUEIMA COELHO DE SOUZA (*in memoriam*)

- DÉBORA BEMERGUY ALVES
- FREDERICO ANTÔNIO LIMA DE OLIVEIRA
- FREDERICO COELHO DE SOUZA (*in memoriam*)
- GUARANY JR
- JEFERSON ANTÔNIO FERNANDES BACELAR
- MAITÊ GADELHA (médica – edição especial)
- MARIA TERESA DA COSTA MACEDO
- DES. MILTON AUGUSTO DE BRITO NOBRE
- PAULO ARTHUR CAVALCANTE KOURY
- RAIMUNDO CHAVES NETO
- ROBERTO VICTOR PEREIRA RIBEIRO
- SÉRGIO ALBERTO FRAZÃO DO COUTO (*in memoriam*)
- DES. MARIA DE NAZARÉ SILVA GOUVEIA DOS SANTOS

PRÊMIO MYRTHES GOMES DE CAMPOS - LISTA DE PREMIADAS

- ROBERTA MENEZES COELHO DE SOUZA (2020)
- MARIA AVELINA IMBIRIBA HESKET (2021)
- ÂNGELA SERRA SALES (2022)
- ANA MARIA RODRIGUES BARATA (2023)
- PAULA FRASSINETTI MATTOS (2024)

COMENDA MARIA ANNUNCIADA CHAVES

- MARIA BETÂNIA FIDALGO ARROYO (2024)

CÁTEDRAS DE INVESTIGAÇÃO CIENTÍFICA DO ISM

I. CÁTEDRA SILVIO MEIRA
II. CÁTEDRA CLÓVIS MALCHER
III. CÁTEDRA DANIEL COELHO DE SOUZA
IV. CÁTEDRA ORLANDO BITAR
V. CÁTEDRA AUGUSTO MEIRA
VI. CÁTEDRA PAULO KLAUTAU
VII. CÁTEDRA OTÁVIO MENDONÇA
VIII. CÁTEDRA ORLANDO TEIXEIRA DA COSTA
IX. CÁTEDRA OCTÁVIO MEIRA

HINO DO INSTITUTO SILVIO MEIRA

Letra e música: José Vicente Malheiros da Fonseca

Nossa fonte do saber,
Entidade cultural
Para o estudo do Direito.

Salve nosso grande jurista!
Mestre do Direito Romano,
Que tanto orgulha o Pará
Tu és universal,
Sílvio Meira imortal,
E nas lições que deixaste,
Não há nada que afaste
Esse nosso ideal.

Sempre em prol da cultura
Base da educação
E na pesquisa, na cátedra,
Da ciência jurídica
Que inspira a canção.

Vamos cantar neste hino
Nosso Instituto querido,
Casa de Sílvio Meira,
Romanista, escritor,
Eternal professor.

Salve nosso grande jurista!
Mestre do Direito Romano,
Que tanto orgulha o Pará

Tu és universal,
Sílvio Meira imortal,
E nas lições que deixaste,
Não há nada que afaste
Esse nosso ideal.

QUEM FOI SILVIO MEIRA?

Silvio Augusto de Bastos Meira, nome literário Silvio Meira, advogado, professor Catedrático e Emérito da UFPA, jurista, jurisconsulto, humanista, germanista, romancista, escritor. Homem de todas as letras. Filho do senador Augusto Meira com Anésia de Bastos Meira, nasceu em Belém do Pará no dia 14 de maio de 1919. Em 1924 iniciou os estudos primários no "Instituto Vieira", concluindo em 1929. No ano seguinte, aos 11 anos, ingressou no Gynásio Paraense (Colégio Paes de Carvalho), onde organizou um jornal intitulado "Nihil", com seis exemplares. Em 1935, aos 16 anos, termina o curso ginasial e realiza o curso pré-jurídico, quando inicia os estudos na língua alemã com a professora Otília Müller Schumann. Aos 18 anos escreve seu primeiro livro, "A conquista do Rio Amazonas", onde conta a história do navegador Pedro Teixeira e, aos 19, escreve seu primeiro romance "Mato Grande", inédito até hoje, quando, também, teve publicado no importante "Jornal do Commercio" um trabalho sobre Frederico Schiller, de sua autoria. Em 1937, ingressa na Faculdade de Direito do Pará. Em 1940, ainda acadêmico de direito, realiza concurso para o Ministério do Trabalho, conquistando o primeiro lugar entre 400 candidatos, assumindo como secretário do Tribunal Regional do Trabalho. Gradua-se em direito no ano de 1942, com o título de "laureado", sendo o orador oficial da turma. Em 1943, desliga-se do Tribunal do Trabalho e é nomeado diretor da Junta Comercial do Estado do Pará. Inscrito na OAB-PA sob o nº 305, foi advogado militante por mais de 30 anos. Completou seus estudos humanísticos em bolsa de estudos na Alemanha, França e Itália, nos anos de 1957 a 1962. Em todas as missões ao exterior manteve contato pessoal com eminentes romanistas, tendo várias de suas obras traduzidas para vários idiomas.

Projetou-se no Pará como legislador (constituinte de 1946), presidente da Comissão que elaborou o projeto da Constituição Política do Estado em 1947 e membro da que elaborou a de 1967, presidente da Comissão de Constituição e Justiça, contribuiu para a redação do Código Civil de 2002, presidente do Instituto dos Advogados do Pará (IAP) e vice-presidente da OAB-PA na gestão de Daniel Coelho de Souza e Egydio Salles. Silvio Meira também foi deputado estadual (líder da maioria), consultor geral da Prefeitura de Belém, consultor geral do Estado, membro do Conselho Estadual (desde a sua fundação em 1969) e do Conselho Federal de Cultura (1971 a 1977), bem como 1º suplente de deputado federal e de senador da República.

Além dos inúmeros cargos que exerceu, era membro de várias entidades culturais, nacionais e estrangeiras, tais como a Academia Brasileira de Letras

Jurídicas (fundador, na cadeira nº 05), Academia Brasileira de História, Instituto dos Advogados Brasileiros (de onde foi Orador Oficial por muitos anos), Instituto Histórico e Geográfico Brasileiro (e de vários Estados, como o do Pará), Academias de Letras (Carioca, Pará, Acre, Paraíba, Alagoas e outras), Academia Brasileira de Literatura Infantil e Juvenil, Sociedade Brasileira de Romanistas, foi presidente da Associação Interamericana de Direito Romano, bem como membro honorário da Academia Paraense de Letras Jurídicas. Com mais de cinquenta títulos e diplomas honoríficos, entre eles o diploma "Al Mérito" da Universidade Autônoma e da Universidade Veracruzana do México, "Palma de Ouro" da UFPA, "Ami de Paris", do Conselho Municipal de Paris, "Medalha do Mérito" da Universidade Federal de Pernambuco, "Medalha Osvaldo Vergara" da OAB-RS, "Medalhas do Centenário de Rui Barbosa", do Centenário de Plácido de Castro, Cidadão Carioca, pela Assembleia Legislativa do Estado da Guanabara, "Medalha José Veríssimo" da Academia Paraense de Letras, "Medalha Cultural Augusto Meira", do Conselho Estadual de Cultura, Diploma de Cidadão Petropolitano e "Prêmio Clio" da Academia Paulista de História (1991), dentre tantos outros. Recebeu quatro prêmios da Academia Brasileira de Letras (Odorico Mendes, Aníbal Freire, Alfredo Jurzikowsky e a mais alta comenda cultural brasileira, a "Medalha Machado de Assis", pelo conjunto da obra). Nas Letras Jurídicas, é o único paraense a receber as três maiores comendas do país: o "Prêmio Pontes de Miranda", da Academia Brasileira de Letras Jurídicas (1980), o "Prêmio Teixeira de Freitas", do Instituto dos Advogados Brasileiros (1971, indicado por 36 juristas) e o "1º Prêmio Brasília de Letras Jurídicas", do Clube dos Advogados do Distrito Federal (1977). Nos anos 70, cursou a Escola Superior de Guerra, sendo orador da turma.

Como professor, em 1947 foi contratado para lecionar Direito Civil e, em 1955, começou a lecionar Direito Romano, conquistando a Cátedra da disciplina em 1958 com a tese "A Lei das XII Tábuas – Fonte do Direito Público e Privado". Em 1989, foi elevado a professor Emérito da UFPA. Silvio Meira, sobretudo, era um germanista. A convite do governo alemão estudou e visitou as universidades de Bonn, Hamburgo, Berlim, Munique, Bochum, Heidelberg, Constanz, Instituto Max Planck, entre outras. Traduziu, do original, a obra-prima "Fausto" de Goethe, em versos rimados (5 edições), merecendo por essa tradução os aplausos de eminentes homens de letras brasileiros. Traduziu, também, o drama "Guilherme Tell", de Frederico Schiller (2 edições), sendo premiado pela Academia Brasileira de Letras. Sobre a cultura tedesca, ainda publicou a bela obra "Estudos Camonianos e Goethianos". Pelas suas realizações no campo germanístico recebeu a mais alta comenda cultural alemã, a medalha "Verdienstkreuz", a Cruz do Mérito da antiga República Federal da Alemanha, em 1ª classe. Sobre a tradução do Fausto feita por Silvio Meira,

escreveu o saudoso Carlos Drummond de Andrade: "Não preciso dizer-lhe do interesse que me despertou a recriação, em vernáculo, da obra-prima alemã, interpretada com tanto escrúpulo intelectual e conhecimento de particularidades literárias, que tornam esse trabalho realmente digno de admiração".

Silvio Meira publicou inúmeras obras nas áreas do Direito, literatura, poesia, ensaio, biografia, tradução e romance, mais de duzentas monografias, artigos e conferências por todo o mundo e mais de quinze mil pareceres jurídicos. Na semana passada já tratamos das obras germanistas, abordando a tradução do "Fausto" de Goethe e o drama "Guilherme Tell", de Schiller, ambas premiadas como a melhores traduções para a língua portuguesa. Aliás, sobre o caráter germanista de Silvio Meira assim pronunciou-se a saudosa escritora Racquel de Queiroz, a primeira mulher a ingressar na Academia Brasileira de Letras: "Silvio Meira é um goethiano, cultor e tradutor do Poeta. Isso se compreende, pois as afinidades entre ambos são evidentes, como a multiplicidade de facetas intelectuais, que no paraense descobrimos na cátedra, na ciência, na linguística, na poesia, no romance. E cada qual tão merecedora de aplausos quanto a obra". Mas, Silvio Meira era, também, um romancista. Sua famosa trilogia "Os Náufragos do Carnapijó", "O Ouro do Jamanxim" e "Os Balateiros do Maicuru", que retratam a vida na Amazônia, eram obras obrigatórias nas escolas públicas do país pelo INL – Instituto Nacional do Livro. Aliás, sobre "O Ouro do Jamanxim", pronunciou-se o grande Carlos Drummond de Andrade: "...belo e vigoroso romance O Ouro do Jamanxim. Ele nos permite visualizar, de forma dramática, a terra e o homem amazônico, através de uma história que cativa o interesse do leitor. Ficção que reflete a vida em movimento, e que por isso, a par do mérito literário, tem o valor de documento social e humano".

No campo da história, Silvio Meira escreveu "A Conquista do Rio Amazonas", "A Epopéia do Acre", "Fronteiras Sententrionais: 3 séculos de lutas no Amapá", "Fronteiras Sangrentas", "Meditações sobre o Fausto de Goethe" (separata) e "Mato Grande" (inédito). Sobre a obra "Fronteiras Sangrentas", assim comentou o saudoso intelectual Gilberto Freyre: "...o erudito admirável, cujo alto saber nunca se desprende das coisas mais nacionais do Brasil, que é o Prof. Silvio Meira". No campo da poesia, publicou "Antologia Poética", "Antologia de Poetas Alemães" (26 poetas), e os ensaios "Estudos Camonianos e Goethianos" – onde faz uma profunda análise comparativa entre o pensamento de Goethe e Camões -, "Andrés Bello e Teixeira de Freitas" e "A missão do orador". Sobre as Antologias Poéticas, assim escreveu o saudoso escritor Octávio de Faria, imortal da Academia Brasileira de Letras: "Silvio Meira é um ser vivo e pulsante, ao mesmo tempo um romancista, e um poeta, um jurista e um ensaísta, um ser que vibra como todos ante tudo o que existe e se faz sentir no tremendo mundo em que vivemos. Apenas, e antes de mais nada, é um ser

voltado para o que há de mais belo e de mais nobre, para o passado mais clássico em cujo culto foi educado – e, digamos assim, esplendidamente educado".

Na área do Direito, foi autor de inúmeras obras, artigos, conferências e trabalhos científicos ao longo da vida, especialmente na área romanista, os quais destacamos: "Curso de Direito Romano" (reeditado em 1996 pela LTr em edição comemorativa), "História e Fontes do Direito Romano", "Instituições de Direito Romano" (um tratado, reeditado em 2017 pelo IASP), "Direito Tributário Romano" (reeditado em 2013 pela Ed. UFPA), "A Lei das XII Tábuas – Fonte do Direito Público e Privado" (sua tese de Cátedra), "Novos e Velhos Temas de Direito", "O Direito Vivo", "Noções Gerais de Processo Civil Romano", "Processo Civil Romano", "Temas de Direito Civil e Agrário", "A vocação dos séculos e o Direito Romano", "Alguns Casos Forenses", "Direitos de ontem e de hoje", "Rui Barbosa na Constituição de 1988", "O Brasil e o Direito Romano", "O Tribunato da Plebe em face do Direito Romano", entre tantos outros. Suas obras foram publicadas pelas melhores editoras do Brasil e do exterior. Notabilizou-se com o lançamento das biografias dos dois maiores juristas do Brasil: "Clóvis Beviláqua – Sua Vida, Sua Obra" e "Teixeira de Freitas – O Jurisconsulto do Império", ambas premiadas, deixando, ainda, a obra "Couto de Magalhães, o último bandeirante" (inacabada). Sobre a biografia de Teixeira de Freitas, assim escreveu o saudoso Afonso Arinos de Melo Franco, titular da cadeira 25 da Academia Brasileira de Letras: "Agora, com este livro monumental sobre Teixeira de Freitas, o humanismo de Silvio Meira adquire nova dimensão, a de biografia, no seu sentido abrangente de ensaio jurídico, pesquisa histórica, reflexão social e compressão humana". Silvio Meira compôs inúmeras bancas de mestrados, doutorados, cátedras e livre docências em diversas universidades da Europa e da América Latina, muitas delas na USP. Em 2017, a Universidade da Amazônia batizou a biblioteca do curso de direito com o seu nome.

Silvio Meira casou-se com Maria José Martins Meira (in memoriam) e teve sete filhos, Aluisio, Maria Silvia, Arnaldo (in memoriam), Heloisa, Celso (in memoriam), Fernando (in memoriam) e Henrique. Dedicou-se também à arte, especializando-se em pintura na França. A música, que ele tão bem retratava no piano "Essenfelder" de cauda longa, também fazia parte dos seus hobbies desde a infância. Falava e escrevia fluentemente mais de oito idiomas, entre eles o latim, alemão, francês, espanhol, italiano, inglês e grego. Silvio Meira faleceu no dia 31 de dezembro de 1995, em Londres/Inglaterra, depois de retornar de uma conferência em Bruxelas. Foi toda uma vida dedicada à cultura, ao trabalho, à família e à pátria.

"Todos nós devíamos nos preparar para o futuro aprendendo coisas que ainda não sabemos, desaprendendo coisas que sabemos, mas não deveríamos mais saber, e reaprendendo coisas que já soubemos e que voltaram a ser úteis."

(Silvio Meira)

Nota das Coordenadoras

A 5ª Edição do Digesto vem cheia de inovação e é uma grande honra e alegria estar coordenando mais essa edição com o apoio, dedicação e vanguardismo do Instituto Silvio Meira, na pessoa de seu presidente André Augusto Malcher Meira.

Falar e escrever sobre Direito Digital e Tecnologia, tem sido muito mais do que pensar em um direito modista, de uma sociedade da informação extremamente conectada, mas, ainda, juridicamente desamparada, considerando o rápido avanço tecnológico que tem afetado todas as esferas do direito, das mais simplórias às mais complexas, das quais possamos pensar e não imaginar.

A inteligência artificial e suas vértices, as questões éticas e morais quanto a sua utilização, os desafios da proteção dos dados diante dos avanços nas áreas como a das famílias, por exemplo, a proliferação das *dark patterns*, o enfrentamento da abordagem de temas como a herança digital, os estudos sobre o metaverso, uso do *phishing* e muitos outros temas atuais e necessários, abrilhantam essa obra que leva o nome do mestre Luiz Paulo Leal da Gama Malcher e conta com grandes autores locais e nacionais.

E pensar em Luiz Paulo Malcher, nome de grande relevância no cenário local e nacional, é exatamente traduzir a ideia de inovação e articulação do direito com a tecnologia.

Ele que foi foi formado em engenharia Civil pela Universidade Federal do Pará (1976), Mestre em Informática pela PUC-RJ (1978), ingressou na UFPA como analista e professor, tendo ocupado a Diretoria de Informática da UFPA (Secom - Serviço de Estatística e Computação), foi cedido para exercer os cargos de Presidente da CINBESA, Diretorias de Informática do Tribunal de Justiça do Estado, Tribunal de Contas do Município e Secretaria de Administração do Estado, exercendo a Presidência da SUCESU-PARÁ e em seguida da SUCESU-NACIONAL e merece o completo reconhecimento de seu valoroso trabalho, através dessa obra cheia de significados, aprendizados e atualidades.

Desejamos a todos uma excelente leitura.

Flávia Figueira
Marina Malcher Gato

Sobre os Autores

ALEXANDRA RODRIGUES DE SOUZA CRUZ
Mestra em Direito pela UNAMA. Especialista em Direito Processual pela UNAMA. Especialista em Psicologia Forense pela Verbo Jurídico. Professora da Graduação e Pós-graduação Latu Sensu em Direito da UNAMA. Assessora de Juiz do Tribunal de Justiça do Estado do Pará.

CAMILY VITÓRIA BORGES DE ANDRADE RIBEIRO
Bacharelanda em Direito pela Faculdade Faci-Wyden.

CLEBER SOARES
Entusiasta de hardware hacking e biohacking, pesquisador em segurança da informação e defensor da cultura do software livre e projetos sustentáveis. Coautor do livro "Introdução à segurança ofensiva: uma abordagem para PenTesters e Red Teams", atualmente, trabalha como Analista de Segurança da Informação, com foco em Análise de Malwares, Resposta a Incidentes, Segurança Ofensiva e Computação Forense. É professor de pós-graduação e instrutor acadêmico. É líder fundador do Capítulo OWASP Belém e autor regular das revistas Hacker Culture, eForenscs Magazine e Hackin9 Magazine.

DEIVISON FRANCO
Mestre em Ciência da Computação. Especialista em Ciências Forenses e em Suporte a Redes de Computadores e Tecnologias Internet. Graduado em Processamento de Dados. Técnico Científico de Tecnologia da Informação do Banco da Amazônia, onde atua como Coordenador de Arquitetura de Tecnologia e Governança de Dados. CEO e Membro Fundador do Grupo de Pesquisas em Segurança da Informação - aCCESS Security Lab. Vencedor do Prêmio Infosec Competence Leaders Brazil 2018/2019 na Categoria "Forensics" e do Prêmio Excelência e Qualidade Brasil 2023 na Categoria

"Profissional do Ano". Membro da Sociedade Brasileira de Ciências Forenses (SBCF) e do IEEE Information Forensics and Security Technical Committee (IEEE IFS-TC). Membro do Corpo Editorial do International Journal of Forensic Sciences (IJFS), da Revista Brasileira de Criminalística (RBC) e do Instituto de Defesa Cibernética (IDCiber). Autor e Revisor Técnico dos livros Tratado de Computação Forense (Millennium Editora), Polícia Científica - Transformando Vestígios em Evidências (Editora InterSaberes), Introdução à Segurança Ofensiva: Uma Abordagem para Pentesters e Red Teams (Editora Brasport) e Fronteiras da Ciência - Coletâne de Debates Interdisciplinares - Volume 3 (Editora Dialética). Autor regular das revistas eForensics Magazine, Hackin9 Magazine, CryptoID e Segurança Digital.

DIEGO MAGNO MOURA DE MORAES

Advogado; procurador Geral do município de Castanhal/PA; professor de Direito Empresarial e Eleitoral na FINAMA; L.L.M/MBA em Direito Empresarial pela Fundação Getúlio Vargas -FGV; Especialista em Startup e Inovações pela Fundação Getúlio Vargas- FGV; Especialista em Direito Eleitoral pela PUC-MG; Mestrando em Direito na UNAMA; e-mail: adv.diegomagno@gmail.com.

FABIANE TRINDADE OZORIO

Bacharelanda em Direito pela Universidade da Amazônia.

FABRÍCIO VASCONCELOS DE OLIVEIRA

Doutor e mestre em Direito pela UFPa; especialista em Direito pelo CEU/SP; professor associado II de Direito Empresarial na Universidade Federal do Pará/UFPa (onde leciona na graduação e no mestrado profissionalizante); professor titular de Direito Empresarial da Universidade da Amazônia/UNAMA (onde leciona na graduação e no mestrado); Procurador Fundacional/Autárquico do Estado do Pará lotado na Junta Comercial do Estado do Pará/JUCEPA; autor de obras jurídicas publicadas em diversos livros e periódicos; email: oliveirafabricio@hotmail.com.

FLÁVIA CHRISTIANE DE ALCÂNTARA FIGUEIRA

Advogada e Professora nas áreas de Famílias e Sucessões e Proteção de Dados e Privacidade, Mestranda do UNICURITIBA/PR, Presidente da Comissão de LGPD do Instituto Brasileiro de Direito das Famílias - IBDFAM/PA, Membro do Understanding IA - USP/PA Membro das Comissões de Famílias e Sucesões OAB/PA e Família e Tecnologia do IBDFAM Nacional, Membro e Diretora da Cátedra de Direito Digital - Instituto Silvio Meira - ISM e Instrutora Convidada da Ópice Blum Academy-São Paulo/SP.

GUILHERME RODRIGUES DE SOUZA CRUZ
Mestre em Uso sustentável de recursos naturais em regiões tropicais pelo Instituto Tecnológico Vale. Pós-graduando em Data Science pela UNAMA. Engenheiro de Controle e automação.

JOAS ANTONIO DOS SANTOS
Um especialista em cibersegurança, possuindo experiência tanto no Red Team quanto no Blue Team, com uma sólida trajetória como pesquisador independente e contribuinte para o MITRE ATT&CK. Com algumas CVEs publicados e mais de 90 certificações internacionais, sou alguém que se dedica à pesquisa e inovação. Atuo em grupos de OSINT, focados em solução contra o combate ao tráfico humano e exploração infantil. Possui presença significativa no mundo acadêmico, sendo autor de diversos artigos com DOI e vários livros sobre cibersegurança e desenvolvimento pessoal. Como palestrante, destaco-me em eventos nacionais e internacionais, compartilhando minhas experiências para enriquecer o campo da cibersegurança. Minha trajetória é marcada por um compromisso contínuo com a educação e inovação, com mais de 200 e-books desenvolvidos para auxiliar profissionais.

JOSÉ ANTÔNIO DE OLIVEIRA ALVES
Mestre em Direito, Políticas Públicas e Desenvolvimento Regional.

LARISSA CLÍSCIA DE SOUZA MENDES VICENTE
Bacharelanda em Direito pela Universidade da Amazônia – UNAMA.

LUISA HELENA CARDOSO CHAVES
Tabeliã e registradora no Estado do Pará, Pós-graduada em Direito Empresarial com concentração em Propriedade Intelectual pela Fundação Getúlio Vargas, Rio de Janeiro/RJ, Diretora na Associação dos Notários e Registradores – Anoreg/PA e na Associação dos Registradores de Pessoas Naturais do Estado do Pará – ARPEN/PA. Membra efetiva no Instituto Silvio Meira – ISM. Mestre em Soluções Alternativas de Controvérsias Empresariais na Escola Paulista de Direito - EPD. Mestranda em Direito pela Faculdade de Lisboa - Portugal. Email:luisachaves1@hotmail.com.

LUIZ EDUARDO GUNTHER
Professor da Graduação e do Programa de Pós-graduação (Mestrado e Doutorado) em Direito do Centro Universitário Curitiba – UNICURITIBA. Doutor pela UFPR; Pós-Doutor pela PUCPR; Desembargador do Trabalho do TRT 9. Membro da Academia brasileira de Direito do Trabalho. E-mail:

luiz.gunther@uol.com.br. Lattes: http://lattes.cnpq.br/1314611892212586. https://orcid.org/0000-0001-7920-3406.

MARCO ANTÔNIO CÉSAR VILLATORE

Professor Concursado Permanente da Graduação e do Programa de Pós-graduação (Mestrado e Doutorado) em Direito da Universidade Federal de Santa Catarina - UFSC. Coordenador da Especialização em Direitos e Processos do Trabalho e Previdenciário da Academia brasileira de Direito Constitucional (ABDConst). Advogado. Membro da Academia brasileira de Direito do Trabalho. E-mail: marcovillatore@gmail.com. Lattes: http://lattes.cnpq.br/6658857270253086. https://orcid.org/0000-0001-6365-6283.

MARIANA PALMEIRA

Advogada, professora da PUC-Rio, doutora em Direito pela PUC-Rio, pesquisadora do Legalite (grupo de pesquisa em direito e novas tecnologias da PUC-Rio) e do Economia Política da Comunicação (EPC - PUC-Rio/CNPq), membro da comissão de privacidade e proteção de dados da OAB-RJ, conselheira suplente do Comitê de Privacidade e Proteção de Dados do Município do Rio de Janeiro.

MARINA PANTOJA

Doutora em Direito do Comércio Internacional e Direito Internacional Econômico - Universidade Paris X, Mestre em Direito Internacional e Direito Europeu- Universidade Paris X, Analista Técnico em comércio internacional na Coordenação Geral de Convergência Regulatória e Barreiras técnicas ao comércio - CGCB-MDIC e Professora universitária.

MAYNARA CIDA MELO DINIZ

Advogada. Bacharel em direito pelo Instituto de Ciência Jurídicas-ICJ na Universidade da Amazônia-UNAMA. Pós-Graduada em Direito Público e Direito de Trânsito pela faculdade LEGALE. Pós-Graduanda em Direito de Família pela faculdade LEGALE. Mestranda em Maestría en Derecho pela Fundação Iboamericana-FUNIBER.

POLLYANNA KRUGER

Advogada e produtora rural. Pós-graduanda em Direito Empresarial (Insper) e em Direito & Economia dos Sistemas Agroindustriais: Regime Jurídico do Agronegócio (IBDA).

RAFAELLA BRANDÃO SOUSA PINHEIRO

Bacharalenda em Direito pela Universidade da Amazônia - UNAMA. LinkedIn: https://www.linkedin.com/in/rafaella-brandao

RICARDO BEZERRA
Pós-graduando em DIREITO DO EXECUTADO pela Ava Educação em Mato Grosso, Advogado, Membro da Academia Brasileira de Direito e da Academia Paraibana de Letras Jurídicas. E-mail: ricardobezerra@ricardobezerra.com.br

SHERLLEN CARVALHO MOREIRA
Administradora e Bacharel em Direito pela Universidade da Amazônia - UNAMA/Grupo Ser, Belém, Pará. Brasil. Pós-Graduanda em Direito Digital e Direito Público e Gestão Financeira pela Facuminas.

SIDNAI ALVES GONÇALVES
Advogada, Especialista em Direito de Famílias e Sucessões. Contato: e-mail: sidnai.alves@gmail.com

THAIS DE SOUZA CARRERA
Discente regularmente matriculado no Curso de Bacharelado em Direito da Universidade da Amazônia sob matrícula nº 04075904. E-mail: thaisscarrera03@gmail.com

VICTOR DE MOURA CARVALHO VALLINOTO
Formado em Direito pela Unama. Membro do IBDFAM. Assessor Consular do Consulado da República Tcheca na Amazônia. Escritor. Historiador.

Sumário

Apresentação

O Instituto Sílvio Meira - Academia de Direito, neste ano de 2024, honrará a memória do saudoso professor **LUIZ PAULO LEAL DA GAMA MALCHER**, falecido em 1º de maio de 2013, mestre em ciências da computação pela PUC/RJ, um dos precursores da informática no estado do Pará, fundador da Tecnoinf – Tecnologia em Informática, uma das empresas pioneiras da computação em Belém, foi um dos fundadores do curso de ciências da computação na Universidade Federal do Pará (UFPA), de onde foi professor, diretor do centro de informática e diretor do DAVES e do SECOM, sendo, também, presidente da Companhia de Informática de Belém (CINBESA), presidente por vários mandatos da SUCESU Nacional e da SUCESU Pará, foi diretor de informática do Tribunal de Justiça do Estado do Pará (TJPA) e do Tribunal de Contas dos Municípios do Estado do Pará (TCM), além de diversos outros importantes cargos públicos que exerceu ao longo da vida.

É uma emoção indescritível coordenar uma obra em homenagem a um tio absolutamente espetacular, que faz todos os dias uma falta irreparável, com quem a vida me deu a oportunidade de começar a trabalhar e dar os meus primeiros passos profissionais e nas salas de aula, tempos absolutamente inesquecíveis de quando eu ainda nem pensava na carreira jurídica, onde aprendi ensinamentos que levarei para o resto da vida, ao lado da imagem e da competência empresarial de Luiz Paulo Malcher. Agradecer ainda às coordenadoras Flávia Figueira e Marina Malcher Gato, pela enorme contribuição e apoio que deram à realização deste sonho.

A inspiração justinianéia perpetuada pelo Digesto original na segunda metade do século VI, resgatou em compilação escrita para o latim e para o grego (Pandectas), a melhor produção científica dos jurisconsultos clássicos, perenizando em cinquenta volumes as bases do melhor conhecimento jurídico

da época, colunas de sustentação do Direito Romano e do moderno Direito Civil, em particular.

À razão do mesmo propósito, de colher e compilar fragmentos da mais respeitada produção intelectual jurídica da atualidade, é que o Instituto Sílvio Meira idealizou um novo DIGESTO, em revista, agora em 5ª edição.

Esta grande obra que homenageia Luiz Paulo Malcher (post mortem) sagra-se ímpar pelo mérito dos articulistas e pela contemporaneidade das abordagens temáticas, encontrou seu escopo e inscreve-se entre as belas obras de arquitetura da genialidade jurídica nacional e internacional. Deleitem-se.

Belém, Pará, Brasil, 13 de setembro de 2024

ANDRÉ AUGUSTO MALCHER MEIRA
Presidente do ISM - Instituto Silvio Meira / Academia de Direito.

Capítulo 1
Lei Geral de Proteção de Dados e seu Impacto nas Relações Familiares

Sidnai Alves Gonçalves
Flávia Christiane de Alcântara Figueira

EVOLUÇÃO DO DIREITO DAS FAMÍLIAS NO BRASIL

Para falar da evolução do direito das famílias no Brasil é imprescindível buscar a origem histórica do conceito romano, que é a base do direito brasileiro.

> A família romana foi organizada de acordo com os princípios do patriarcado, tendo como figura central o *paterfamilias,* com grandes poderes sobre os que lhe eram subordinados. (MEIRA, 2017, p.130)

O que significa dizer que a família compunha o patrimônio que pertencia ao *pater* e cujo poder era por ele exercido exclusivamente sobre todos os descendentes, sendo repassado ao herdeiro mais velho, após a morte do antecessor, para que o exercesse da mesma forma.

> Na família romana, *sui juris* era aquele cuja capacidade jurídica não sofria quaisquer restrições: o *paterfamilias.* Agia por si, exercia o *jus commercii, o jus connubii, o jus suffragii, o jus honorum*, possuía a *testamenti factio* ativa e passiva, sem quaisquer restrições. (MEIRA, 2017, p.136)

Foi esse modelo de família e necessidade de manutenção do patrimônio que deu origem ao Código Civil brasileiro de 1916, que era voltado para a perpetuação de um regime patriarcal e patrimonialista, onde tudo girava em torno do querer masculino, sendo a mulher considerada, inclusive, relativamente incapaz e necessitava da autorização do marido para o exercício de qualquer ato civil.

> A noção clássica de família consagrada no Código Civil então vigente, que representava a transição para o século XX, ou da Colônia para a República, era patriarcal, hierarquizada, transpessoal, matrimonializada e patrimonializada. Tratava-se de uma estrutura moral e social, mais do que sentimental. (ROSA, 2013, p. 26)

A sociedade brasileira começa a ganhar novos contornos a partir da Constituição Federal de 1988, que possibilita grandes avanços sociais em nosso ordenamento jurídico, trazendo vários dispositivos fundamentais para a garantia de direitos, tais como a igualdade entre homens e mulheres, entre os filhos sejam eles oriundos ou não da união conjugal, dentre outros (MADALENO, 2018).

> A Carta Magna acolheu as transformações sociais da família brasileira e reconheceu a igualdade dos cônjuges e dos filhos, bem como outras formas de constituição de família fora do casamento, não recepcionando as normas que prevaleciam no Código Civil de 1916, o que exigiu sua atualização nas leis especiais, inclusive com a edição de novas normas. (ROSA, 2013, p. 34)

Desse modo, para Maria Berenice Dias (2017), a família passa a ser definida na Constituição como sendo a base da sociedade, merecendo proteção do Estado, a partir de princípios norteadores para a consolidação do Direito das Famílias.

> Não bastou a Constituição proclamar o princípio da igualdade em seu preâmbulo. Reafirmou o direito à igualdade ao dizer (CF 5º): todos são iguais perante a lei. E foi além. De modo enfático, foi até repetitiva ao afirmar que homens e mulheres são iguais em direitos e obrigações (CF 5º, I), decantando mais uma vez a igualdade de direitos e deveres de ambos no referente à sociedade conjugal (CF 226 § 5º). Assim, é a carta constitucional a grande artífice do princípio da isonomia no direito das famílias. Foi banida a desigualdade de gêneros. A supremacia do princípio da igualdade alcançou também os vínculos de filiação, ao ser proibida qualquer designação discriminatória com relação aos filhos havidos ou não da relação de casamento ou por adoção (CF 227 § 6.º). (DIAS, 2017, p.54)

De acordo com Maria Berenice Dias (2017), os princípios constitucionais mudam de categoria quando passam a ter eficácia imediata, sendo alçados ao patamar de valores fundamentais no momento da correta interpretação e aplicação das leis. Portanto, esses princípios, quando acoplados à realidade social brasileira, tem propiciado uma releitura de Direito das Famílias.

> Embora seja verdade que a Constituição Federal foi revolucionária ao expandir o conceito oficial de família e permitir o reconhecimento de outros modelos de relação familiar que não fosse obrigatoriamente ligados ao casamento,

> e diante dessa realidade estender à união estável e à família monoparental o mesmo braço protetor destinado ao matrimonio (CF, art. 226), não é possível desconsiderar a pluralidade familiar e de cujo extenso leque o Estatuto da Criança e do Adolescente, com a incorporação dessa filosofia pluralista, reuniu em texto escrito o reconhecimento oficial de diferentes modelos de núcleos familiares: como a família natural, família ampliada e a família substituta. (MADALENO, 2018, p. 44)

O Código Civil de 2002 foi muito importante para evocar as mudanças já trazidas pela Constituição Federal de 1988. Dentre as mais significativas para o Direitos das Famílias está a igualdade dos cônjuges na relação familiar, com a extinção do poder patriarcal, bem como a dissolução do vínculo conjugal através da separação e do divórcio, além da igualdade entre os filhos, sejam eles de sangue, advindos ou não do casamento e os adotados, bem como o surgimento do instituto da união estável. Tudo isso evidenciando que são diversas as modalidades de famílias, sejam formadas pelas relações sanguíneas, atos jurídicos ou pela socio afetividade.

> Na era da despatrimonialização do Direito Civil, que elevou a dignidade da pessoa humana a fundamento das constituições democráticas, toda ordem jurídica deve ter o seu foco na pessoa, em detrimento do patrimônio, que antes comandava todas as relações interprivadas. Família, afinal, é o lugar privilegiado da realização da pessoa, pois é aí que se inicia e se desenvolve todo processo de formação da personalidade do sujeito. A família deixou, portanto, de ser um núcleo econômico e de reprodução para ser o espaço do amor e do afeto. (ROSA, 2013: 40).

É importante destacar que o direito das famílias tem uma natureza profundamente dinâmica que, na maioria das vezes, não é acompanhado pela atualização legislativa, já que a norma acaba tendo um aspecto conservador, refletindo as características sociais em que está inserida.

> O influxo da chamada globalização impõe constante alteração de regras, leis e comportamentos. No entanto, a mais árdua tarefa é mudar as regras do direito das famílias. Isto porque é o ramo do direito que diz com a vida das pessoas, seus sentimentos, enfim, com a alma do ser humano. O legislador não consegue acompanhar a realidade social nem contemplar as inquietações da família contemporânea. A sociedade evolui, transforma-se, rompe com tradições e amarras, o que gera a necessidade de oxigenação das leis. (DIAS, 2017, p.39)

Portanto, a evolução social, que rompe com preconceitos e dogmas já superados, implica na necessária atualização normativa, para que haja o acompanhamento da sociedade atual.

> Uma das grandes evoluções do pensamento contemporâneo, com a ajuda da antropologia e da psicanálise, foi ter trazido a compreensão de que a família não é um fato da natureza, mas da cultura. E se a família é um fato cultural, ela pode sofrer variações de acordo com o tempo e o espaço. Ou seja, cada sociedade, cada cultura, podem construir diferentes formas de família. Caberá aos ordenamentos jurídicos fazer as adequações para regular e proteger direitos e deveres decorrentes destas relações. (ROSA, 2013, p. 23)

Desta forma, Rosa destaca que a família sempre será o núcleo central de toda sociedade e sem ela nenhuma organização social ou jurídica prosperará, uma vez que é nela, família, que tudo começa, onde nos construímos enquanto sujeitos e encontramos amparo e esteio emocional.

A LGPD E A SUA IMPORTÂNCIA

Para tratar da Lei Geral de Proteção de Dados é necessário o desvelamento da sua relevância a partir da construção de um referencial teórico apto a explicitar o que seria esse direito à privacidade e à proteção de dados pessoais.

O direito à privacidade destaca-se na legislação brasileira desde a Constituição Federal de 1988, inspirada na Declaração Universal dos Direitos Humanos de 1948, trazendo como direitos a serem tutelados pelo Estado a inviolabilidade da vida privada, da intimidade, da imagem e da honra.

Da mesma forma, a proteção de dados pessoais está diretamente ligada com os direitos da personalidade, entendidos por Gagliano e Pamplona Filho, como sendo "os direitos da personalidade como aqueles que têm por objeto os atributos físicos, psíquicos e morais da pessoa em si e em suas projeções sociais" (2010, p. 182). Portanto, o direito personalíssimo está intrinsicamente vinculado à proteção de dados e à privacidade, que por sua vez manifesta-se por meio do direito à intimidade.

Porém, é importante destacar que existe uma diferença entre o direito à privacidade, compreendido como tudo que está relacionado à vida particular do indivíduo, atrelado à intimidade e que deve de modo geral ficar restrito à vontade pessoal. Já o direito à proteção de dados, diz respeito às informações pessoais, que podem ser públicas ou privadas e que são captadas com uma finalidade específica, devendo tais dados passar por tratamento para que tenha seu uso restrito à finalidade original.

> Logo, a privacidade hoje, longe de se restringir à intimidade e ao direito de ser deixado só, ampliou seus domínios para abranger o controle sobre as informações que digam respeito ao sujeito, a autodeterminação informativa, o direito à não discriminação, a liberdade, a igualdade, o direito ao acesso e acompanhamento dos dados pessoais quando se tornam objeto de disponibilidade de outros, dentre outros. (FRAZÃO, 2019, p. 109)

Mesmo antes da implementação da LGPD já existiam espalhadas em algumas legislações brasileiras a determinação sobre a proteção de dados, mas não com a evidência e importância trazida pela referida lei. Dentre as principais podemos destacar a Lei 8.519/91 de Arquivos Públicos, a Lei 12.572/2011 de Acesso à Informação e a que merece um destaque por sua relevância que é a Lei 12.965/2014 e ficou conhecida como Marco Civil da Internet e tratava dos princípios, garantias, direitos e deveres para regulamentação do uso da internet no Brasil.

> Faltava, contudo, maior especificidade e centralidade no que diz respeito à abordagem frente aos dados pessoais, ou seja, às informações pessoais que determinam a identificação, ou possibilidade de identificação, de uma pessoa, como seu nome, data de nascimento, número de cédula de identidade, entre outros. (CELANO e ESPERATO, 2020, p. 17)

A LGPD, surge inspirada na legislação europeia *General Data Protection Regulation* (GDPR) e se fundamenta na autodeterminação informativa, propiciando aos titulares dos dados pessoais o poder de controlar suas informações e os seus dados. Dispõe sobre as regras de coleta, armazenamento, tratamento e compartilhamento de dados pessoais, compreendidos como sendo todas as informações relacionadas a pessoa natural identificada ou identificável e aos dados sensíveis, inclusive nos meios digitais, objetivando a proteção da liberdade e da privacidade dos indivíduos.

> Longe de ser um instrumento de proteção apenas da privacidade, pelo menos no sentido tradicional a ela atribuído, a lei pretende proteger diversas situações existenciais da mais alta importância. (FRAZÃO, 2019, p. 99)

Em seu Artigo 1º, a LGPD afirma que:

> 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.

Neste sentido, podemos entender a LGPD como sendo uma regulamentação do uso dos dados pessoais, aqui entendido como sendo toda informação relacionada à pessoa natural identificada ou identificável, em uma contextualização caracterizada pela pertinência das informações pessoais.

> A utilização de dados pessoais não é, em si, um problema. Na verdade, ela torna possíveis várias atividades, desde o planejamento administrativo até a ação humanitária, passando pela pesquisa de mercado e por mais um número

> infindável de áreas. Ocorre que a atividade do tratamento de dados pessoais requer instrumentos que a harmonize com os parâmetros de proteção da pessoa humana presentes nos direitos fundamentais e funcionalizados por instrumentos regulatórios que possibilitem aos cidadãos um efetivo controle em relação aos seus dados pessoais, garantindo o acesso, a veracidade, a segurança, o conhecimento da finalidade para a qual serão utilizados, entre tantas outras garantias que se fazem cada vez mais necessárias. (DONEDA, 2019, p. 24)

Com a promulgação da Emenda Constitucional nº 115, em 10 de fevereiro de 2022, a proteção de dados pessoais passou a ser um direito fundamental, com a União sendo a responsável pela legislação da proteção e tratamento de dados pessoais, o que certamente foi um avanço para a implementação da LGPD no país. (SIROTHEAU, 2022).

Destarte, a privacidade, entendida como direito personalíssimo, sofre violação quando os dados pessoais são vazados ou utilizados sem autorização de seu titular, seja para qual for a finalidade.

O IMPACTO DA LGPD NAS RELAÇÕES FAMILIARES

Apesar de aparentemente não haver ponto de conjunção entre a LGPD e as relações familiares, acreditamos que esses dois institutos estão diretamente vinculados, quando as famílias são compostas por indivíduos titulares de dados pessoais, que carecem de uma educação voltada para a cultura da proteção desses dados sensíveis.

> A começar pelo fato de que a garantia dos direitos de personalidade e do resguardo do interesse de menores e incapazes estão abrigados pela área do Direito das Famílias e, também, são diretamente disciplinados pela LGPD. Está aí o ponto de intercessão entre a LGPD e as relações familiares. (SANCHES e LAMOSA, 2021, p. 38)

Os núcleos familiares são cerne de proteção à intimidade, sendo constantemente submetidos ao risco de violação de sua privacidade pelo acesso à tecnologia gradativamente mais frequente, principalmente se considerarmos que estamos inseridos em um ambiente cada vez mais tecnológico. Sanches e Lamosa asseguram que,

> O ambiente doméstico-familiar é o mais privativo. É na intimidade do lar que se encontra a proteção da privacidade, onde são despidas as vestes sociais e os diplomas são de mera decoração – âmbito dos segredos e onde residem os desejos, onde os sonhos são formados. Portanto, o ambiente doméstico é onde o indivíduo se encontra mais vulnerável e, por essa razão, a violação da intimidade doméstica é tão fortemente rechaçada. (SANCHES e LAMOSA, 2021, p. 38)

Se consideramos que a tecnologia está cada dia mais presente em nossas vidas, seja através do uso de smartphones, computadores ou de eletrodomésticos dotados de inteligência artificial e conectados à internet, os dados pessoais ficam disponíveis através da necessária permissão para utilização dos aplicativos correspondentes. É justamente nessa necessidade de compartilhamento de informações que o perigo de vazamento de dados sensíveis se faz presente.

> a disciplina do consentimento não deve ser tratada sob viés negocial, mas sim a partir do poder de autodeterminação e a consideração dos direitos fundamentais em questão. (DONEDA, 2006, p. 410)

É nesse ambiente familiar que a vulnerabilidade se instala e os dados pessoais e familiares ficam disponíveis para serem coletados e comercializados sem o consentimento dos seus titulares.

> Os problemas que decorrem da exploração dos dados pessoais são muito mais extensos do que a mera violação da privacidade, especialmente se tal direito for compreendido sob a sua acepção clássica, ou seja, no sentido de intimidade e do direito de ser deixado só. Além da privacidade, há vários outros desdobramentos da personalidade que são colocados em risco pela economia movida a dados, como a própria individualidade e autonomia. Mais do que isso, não é exagero afirmar que a própria democracia também passa a estar sob ameaça. (FRAZÃO, 2019, p.100)

Daí a importância da LGPD, quando em seu Art. 14 afirma que:

> O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente. § 1º 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.

Este dispositivo ainda que verse exclusivamente sobre o tratamento de dados de crianças, deve ser lido extensivamente para os adolescentes também, se considerarmos que estes são juridicamente incapazes de praticar atos da vida civil.

> Ora, pela regra do art. 14, §1º, os adolescentes não precisariam dar expressa anuência para coleta e tratamento de dados. Com isso, os impúberes (entre 12 e 16 anos) estariam aptos, conforme a lei, para consentir sem a representação paterna e os relativamente incapazes (entre 16 e 18 anos), da mesma forma, não precisariam de assistência dos pais ou responsável legal. (FALEIROS JÚNIOR e DIRSCHERL, 2022, p. 356)

Pesquisa realizada no ano de 2020, com 6,3 mil crianças e adolescentes com idades entre 9 e 17 anos em todas as regiões do país na intencionado orientar sobre o uso da tecnologia, desenvolvida pela Secretaria Nacional dos Direitos da Criança e do Adolescente (SNDCA), do Ministério da Mulher, da Família e dos Direitos Humanos (MMFDH), em parceria com a entidade civil Viração Educomunicação e analisada por Teixeira, Faleiros Júnior e Densa (2022), apontou que:

> 86% das crianças e adolescentes usam a internet diariamente e 80% da faixa etária até 12 anos informou acessá-la no mínimo uma vez por dia. Do total que "não usa", 15% vivem em área rural e 2,5% em área urbana.
> Para 51% dos entrevistados, os adolescentes se abrem mais na internet do que com os pais. Para completar, 46% afirmam que, se tivessem mais atenção da família, passariam menos tempo no celular. Dentre outras constatações, a pesquisa aponta que 66% das crianças declararam ter começado a usar as redes sociais antes dos 12 anos, inclusive indicando idades maiores para fins de conseguirem acesso a um perfil pessoal. Por outro lado, apenas metade dos entrevistados informou que possui algum tipo de supervisão dos pais ou responsáveis durante as atividades realizadas na internet. (TEIXEIRA, FALEIROS JÚNIOR E DENSA, 2022: 11)

Dada a vulnerabilidade e suscetibilidade de crianças e adolescente constantemente expostas na internet, é imprescindível o desenvolvimento de uma cultura de proteção de dados pessoais, viabilizada pela educação digital, que abranja todos os sujeitos do núcleo familiar, principalmente os mais vulneráveis, como crianças, adolescentes e idosos, que estão constantemente se atualizando e fazendo uso das tecnologias.

> Trata-se de atuação dos pais para orientar seus filhos, crianças e adolescentes, para a compreensão da importância da segurança na Rede, navegando de forma saudável e segura no ambiente virtual. São condutas dos pais para preparação dos filhos para o mundo tecnológico. (TEIXEIRA e MULTEDO, 2022, p. 31)

Segundo dados da Pesquisa Nacional por Amostra de Domicílios Contínua – PNAD Contínua, do ano de 2019, divulgada pela GERO360, os idosos cada vez mais estão inseridos no universo digital, seja através das redes sociais ou como ferramenta de consumo de produtos e serviços.

> Um recorte sobre a tecnologia mostra que os idosos estão cada vez mais conectados e interagindo socialmente nos meios digitais. Por exemplo, segundo pesquisa da PNAD Contínua, eles formam o grupo que mais cresce entre usuários da internet no Brasil – um em cada quatro brasileiros acima dos 60 anos já está na internet. O mesmo se aplica ao Facebook, de acordo com

> um levantamento da consultoria Senior Lab. Não apenas para conexão social, este grupo utiliza a internet para aprender novas atividades, fazer serviços bancários, comprar online, acompanhar notícias, jogar. Além disso, uma pesquisa feita pelo Serviço de Proteção ao Crédito (SPC) mostra que o poder de consumo da população de +50 no Brasil equivale a R$ 1,6 trilhão por ano. Ainda que direcione seus gastos com o cuidado da saúde e medicamentos, esta parcela da população também direciona seus gastos para o uso do cartão de crédito, compra de automóveis, perfumaria e cosméticos, higiene pessoal, roupas e acessórios. (GENRO360, 2019)

Desta maneira, a orientação sobre os cuidados com o acesso à internet deve ser direcionada também para os idosos, assim como as crianças e adolescentes, através do entendimento de que é preciso manter atenção no acesso à rede e aos meios de tecnologia sem supervisão e orientação, pois além de coloca-los à mercê dos perigos virtuais, também os coloca em posição de risco de vazamento de dados familiares que possam gerar danos diversos.

> É nesse sentido que uma lei geral de proteção de dados, tal como a LGPD brasileira, pretende reequilibrar essas forças, aumentando o protagonismo por parte do titular de dados pessoais. O que está em jogo não é apenas a privacidade no sentido da intimidade, mas, também, a autonomia informativa e o controle sobre a informação, assim como uma série de questões relacionadas à igualdade e à própria liberdade, cuja tutela é imprescindível tanto sob a ótica individual, como sob a ótica social, considerando que as bases da democracia hoje dependem igualmente da regulação de dados. (FRAZÃO, 2019, p. 127)

É preciso entender que cada vez que concordamos com alguma solicitação feita por aplicativos ou sites na internet, estamos dando a alguém a permissão para a coleta e armazenamento de nossos dados pessoais e, com isso, nos colocamos em posição de vulnerabilidade. Não só a quem o faz, mas a toda a família. Por isso é tão necessária uma lei como a LGPD que regulamenta o tratamento dos dados pessoais.

Partindo desse entendimento, o Artigo 55-J, inciso XIX da LGPD estabelece a competência da Autoridade Nacional de Proteção de Dados (ANPD), que visa assegurar que o tratamento de dados de pessoas idosas seja realizado de forma simples, clara, acessível e adequada ao seu entendimento, conforme disposto tanto na referida lei quanto no Estatuto do Idoso.

Observa-se, portanto, que o legislador buscou harmonizar as regras de tratamento de dados da pessoa idosa estabelecida pela LGPD com os princípios de proteção estipulados no Estatuto do Idoso.

No entanto, não se pode presumir que apenas a lei seja capaz de solucionar todos os problemas inerentes à proteção de dados pessoais, principalmente se considerarmos que a heterorregulação acerca dos dados pessoais é assunto

complexo e demanda empenho de todos os envolvidos na seara da proteção de dados.

REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Dispõe sobre a Proteção de Dados Pessoais** e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 15 ago. 2018, n. 157, Seção 1, p. 59.

DIAS, Maria Berenice. **Manual de direito das famílias** – 12 ed. São Paulo: Editora Revista dos Tribunais, 2017

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

DONEDA, D. A. A proteção de dados pessoais nas relações de consumo: para além da informação creditícia. Brasília: SDE-DPDC, 2010. Disponível em: https://www.defesadoconsumidor.gov.br/images/manuais/vol_2_protecao_de_dados _pessoais.pdf. Acesso em: 18 abr. 2022.

FRAZÃO, Ana; TEPEDINO, Gustavo e OLIVA, Milena Donato, coordenação. **A Lei Geral de Proteção de Dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

GAGLIANO, P. S; PAMPLONA FILHO, R. Novo curso de direito civil: parte geral. 12. ed. São Paulo: Saraiva, 2010.

GENRO360. O idoso no Brasil: entenda o envelhecimento hoje no país. 2019.

MADALENO, Rolf. **Direito de família** – 8 ed. Rio de Janeiro: Forense, 2018

MEIRA, Silvio Augusto de Bastos. **Instituições de Direito Romano.** São Paulo: Editora IASP, 2017.

ROSA, Conrado Paulino da. **IFamily: um novo conceito de família?** São Paulo: Saraiva, 2013.

SANCHES, Patrícia Corrêa; DIAS, Maria Berenice; PEREIRA, Rodrigo da Cunha. Organizadores. **Direito das famílias e sucessões na era digital.** Belo Horizonte: Instituto Brasileiro de Direito de Família – IBDFAM, 2021

SIROTHEAU, Débora. Com a promulgação da Emenda Constitucional 115, a Proteção de Dados é agora um direito fundamental. FENADADOS. Disponvel em: Com a promulgação da Emenda Constitucional 115, a Proteção de... – Fenadados Acesso em: 18 de nov. 2022

TEIXEIRA, Ana Carolina Brochado; FALEIROS JÚNIOR, José Luiz de Moura; DENSA, Roberta (coordenadores). **Infância, Adolescência e Tecnologia: o Estatuto da Criança e do Adolescente na Sociedade da Informação.** Indaiatuba, SP: Editora Foco, 2022.

Capítulo 2

Herança Digital e os Desafios de Regulamentação no Ordenamento Jurídico no Âmbito Familiar Entre Cônjuges no *Post Mortem*

Larissa Clíscia de Souza Mendes Vicente
Flávia Christiane de Alcântara Figueira

INTRODUÇÃO

O presente artigo trata sobre ativos digitais, mais especificamente sobre a herança digital no direito sucessório, ou seja, a herança de bens digitais, apresentando os desafios na regulamentação e a falta de legislação acerca da transmissibilidade no *post mortem*. Diante desse cenário, investiga-se: Como o ordenamento jurídico deve se posicionar acerca do partilhamento de bens digitais entre os cônjuges, assegurando umtratamento equitativo tanto aos ativos digitais quanto aos patrimônios convencionais, sem a violação da privacidade e da personalidade.

Assim, o presente artigo visa mostrar a urgente necessidade de regulamentação de normas no ordenamento jurídico brasileiro acerca das diretrizes da sucessão dos bens digitais deixados em ambiente virtual, haja vista a inexistência de legislação testamentária no Brasil sobre a temática.

O patrimônio digital sucessório já é uma realidade, assim como a tutela da transmissibilidade da herança no Brasil. Sua relevância está intrinsecamente ligada ao conceito de direito sucessório, que engloba um conjunto de normas legais relacionadas à transferência de patrimônio de um indivíduo após o seu falecimento.

Surgindo, assim, várias indagações sobretudo a respeito da destinação desses bens após a morte do seu titular.

Nesse sentido, será analisada a emergência de se legislar sobre bens sucessórios digitais, sem que ocorra violação de privacidade e de personalidade. Será utilizada metodologia dedutiva e estudos bibliográficos. Concluindo, ao final, pela importância de uma adequada legislação para que se

obtenha maior segurança jurídica aos direitos dos herdeiros, mas também que preserve a honra, a intimidade e a privacidade do *de cujus.*

1. HERANÇA DIGITAL E ATIVOS/BENS DIGITAIS: CONCEITOS E COMPLEXIDADES

Ao abordamos a temática acerca da herança digital, temos que a herança digital se refere ao conjunto de bens e ativos digitais intangíveis que uma pessoa acumula durante sua vida.

Nesse sentido, cabe-nos classificar os bens digitais em três grupos distintos: patrimoniais, existenciais e patrimoniais-existenciais.

Bens digitais patrimoniais com valorações econômicas, os quais são: contas de mídias sociais, vídeos, músicas, criptomoedas, registros financeiros, milhas aéreas e outros conteúdos online. Por serem de natureza virtual e frequentemente protegidos por senhas e mecanismos de segurança, apresentam desafios específicos no contexto sucessório. Os bens digitais patrimoniais são aqueles de predominância econômica por gerarem consequências de ordem financeira, portanto presume-se que eles devem compor o patrimônio como bens na sucessão.

Passemos, agora, aos bens digitais existenciais ou personalíssimos, que são aqueles que carregam um valor existencial e são preservados em sistemas de armazenamento tipo "nuvem", como Dropbox, Icloud e OneDrive, bem como em servidores descentralizados. Os bens digitais existenciais são de origem pessoal e contêm informações particulares do falecido. Alguns exemplos desse tipo de bem: arquivos de fotografias pessoais em "nuvens" ou redes sociais, vídeos pessoais, correspondências virtuais trocadas com terceiros por meio de e-mails ou por outros serviços de aplicativos de mensagens.

E, por fim, podemos citar os bens híbridos, que possuem tanto características patrimoniais quanto existenciais. Isso ocorre à medida que o conteúdo é inserido no ambiente virtual pelo titular e desperta interesse nos outros, passando, assim, a gerar valor monetário. Estão inseridos nessa categoria, os perfis em redes sociais. É o que acontece com criadores de conteúdo em plataformas como YouTube, X (anteriormente conhecido como Twitter), TikTok, Kwai e Instagram.

Conceituando essa afirmação, Zampier (2017) no diz que bens digitais podem ser definidos como "bens incorpóreos, os quais são progressivamente inseridos na Internet por um usuário, consistindo em informações de caráter pessoal que lhe tragam alguma utilidade, tenham ou não conteúdo econômico".

Assim, diante de uma interpretação extensa, pode-se afirmar que herança digital é "o patrimônio digital deixado pelo autor da herança" (Bizerra, 2021).

Complementando o mesmo âmbito doutrinário da temática, Xisto (2018) conceitua a herança digital como:

> Universalidade de bens adquiridos pelo *de cujus*, em formato digital, podendo estar inserido no software de uma plataforma digital, como por exemplo, o computador e o smartphone, ou armazenados na internet, através de contas em redes sociais, vídeos, fotos, documentos, que possuem valor econômico, sentimental ou informacional, e que poderão ser passiveis de transmissão em decorrência da morte do seu titular.

A controvérsia e a complexidade da herança digital decorrem, em grande parte, da interação entre a legislação tradicional de sucessões e as políticas de privacidade e segurança impostas por empresas de tecnologia. A legislação existente não aborda especificamente a questão da herança digital, o que leva a lacunas legais e dificuldades práticas para os herdeiros.

2. HISTÓRICO ACERCA DAS NOVAS TECNOLOGIAS DA INFORMAÇÃO

Atualmente quase tudo está ao alcance de um clique ou na palma da mão com a utilização de smartphones e de outras tecnologias de informação por meio da internet. E foi nesse contexto que surgiram indagações acerca dos conflitos sociais e jurídicos dos bens específicos do universo digital. Nesse cenário, a informação se tornou uma ferramenta de comunicação e grande mediadora das relações sociais. E a sociedade se percebeu na criação de um acervo que engloba fotos, músicas, milhas aéreas, perfis de redes sociais, canais em plataformas, dentre outros exemplos de bens digitais acumulados no cenário digital.

Não se pode falar em herança digital sem conceituar direito sucessório. Vejamos o que a Lei nº 10.406, de 10 de janeiro de 2002, que institui o Código Civil, traz sobre o direito sucessório:

> Livro V - Do Direito das Sucessões Título I - Da Sucessão em Geral [...] Título II - Da Sucessão Legítima [...]
> Título III - Da Sucessão Testamentária [...]
> Título IV - Do Inventário e da Partilha (Brasil, 2002)

Dessa forma, há duas maneiras de ocorrer a sucessão, por lei ou por ato de última vontade. A sucessão que decorre da lei é a sucessão legítima, e a que se origina do ato de última vontade é a sucessão testamentária.

Segundo Tartuce (2016), "a ordem de raciocínio a ser seguida na sucessão é de primeiro investigar a existência de disposição de última vontade que seja válida e eficaz. Não havendo tal disposição testamentária, vige a ordem de sucessão legítima estabelecida por lei".

Sobre testamento, vejamos o que Souza e Siqueira (2023) têm a dizer:

> O testamento para o Código Civil, nos artigos 1.862 a 1.880 é o ato mais formal pelo qual alguém dispõe sobre a totalidade ou parte de seu patrimônio para após sua morte. Pode ser público, cerrado ou particular, nas formas ordinárias, bem como marítimo, militar e aeronáutico, nas modalidades extraordinárias, abrangendo disposições patrimoniais e não patrimoniais.

Já o codicilo, identificado nos artigos 1.881 e 1.885 do Código Civil, é uma forma mais simples de disposição testamentária.

A herança digital é um tema recente, daí a necessidade de que se discuta sobre essa temática. Logo, Lara (2016) nos diz:

> No tocante à herança digital, será necessária uma lei específica para regrar diretamente o tema, seguindo os princípios traçados pela Constituição Federal e pelo Marco Civil da Internet, mas acrescentando dispositivos legais no Código Civil, de forma que o cidadão brasileiro tenha o seu direito à herança de bens digitais explicitados na lei e dessa maneira plenamente assegurados.

A discussão se concentra na definição dos direitos dos herdeiros em relação aos bens digitais, especialmente quando o acesso é protegido por senhas e mecanismos de autenticação.

Na atualidade, a legislação brasileira não aborda explicitamente a questão da herança digital, nem o Código Civil, nem o Marco Civil da Internet (Lei nº 12.965/2014), nema Lei Geral de Proteção de Dados - LGPD (Lei nº 13.709/2018) tratam do assunto. Nesse enquadramento, o testamento, uma ferramenta consagrada no direito brasileiro, emerge como um meio significativo para proteger o patrimônio digital. Contudo, sua adequação se faz imperativa para atender às peculiaridades e aos desafios impostos pelo ambiente digital.

Vindo ao encontro desse entendimento, o Enunciado 687 do Conselho de Justiça Federal nos diz que: "O patrimônio digital pode integrar o espólio de bens na sucessão legítima do titular falecido, admitindo-se, ainda, sua disposição na forma testamentária ou por codicilo" (Brasil, [2022]).

Tanto o Enunciado 40 como o Enunciado 687 do referido Conselho, servem de orientação doutrinária no entendimento do Poder Judiciário acerca da destinação dos bens digitais.

A partir de lacunas legislativas, verifica-se o conflito entre o direito à herança dos ativos digitais pelos sucessores e os direitos da intimidade do falecido. A Constituição Federal nos diz, em seu artigo 5°, inciso X, 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" (Brasil, 1988).

3. REGULAMENTAÇÃO DOS BENS DIGITAIS

A inquietação na preservação e destinação dos bens digitais demostra a urgência em se encontrar uma solução correta para esses ativos. Diante dessas considerações, percebe-se que a jurisprudência avalia a temática como emergente no mundo jurídico, impulsionada pelo avanço da tecnologia e pela presença digital em nossas vidas.

Dessa forma, como nos diz Augusto e Oliveira (2015):

> Os bens digitais estão cada vez mais presentes no cotidiano de nossa sociedade, e mesmo que não exista regulamentação específica pela legislação, são aceitos na ordem jurídica interna, haja vista que fazem parte como subespécies de bens incorpóreos, devend o assim receber a mesma proteção jurídica que estes recebem.

Devido à necessidade de acompanhar a evolução do ambiente contemporâneo a este mundo digital e evitar possíveis embates nos tribunais, muitas empresas têm adotado alguns critérios acerca de gerenciamento de conta: além de sites especializados, existem também dispositivos que permitem o gerenciamento da conta do usuário após sua morte, ou seja, podem eleger contatos de legado, designar pessoas de confiança às quais caberá gerenciar os dados de sua conta em caso de morte. Salientamos, também, que os dados do usuário de conta pessoal associada ao aparelho celular são tutelados pela Lei nº 13.709/18, Lei Geral de Proteção de Dados (LGPD), norma que protege o direito à privacidade e à inviolabilidade da intimidade, da honra e da imagem.

Ademais, a Lei nº 12.905/14 estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. E, em seu artigo 7°, inciso III, prevê que são assegurados o sigilo e a inviolabilidade da comunicação privada armazenada, salvo por ordem judicial (Brasil, 2014).

Atualmente, fica a critério das plataformas a destinação sobre o que é feito com os perfis e bens digitais considerando regras contratuais, salvo as disposições de última vontade do falecido em testamento.

A Autoridade Nacional de Proteção de Dados (ANPD) declarou que a Lei Geral de Proteção de Dados não é aplicável a dados de pessoas já falecidas, haja vista que a personalidade jurídica de uma pessoa cessa com a sua morte, conforme o artigo 6° do Código Civil (Brasil, 2002).

4. O DEBATE JURÍDICO EM TORNO DA HERANÇA DIGITAL POST MORTEM E O POSICIONAMENTO DOS TRIBUNAIS

Nos tribunais brasileiros, encontram-se várias decisões que juridicamente validam os bens digitais. Além dos artigos jurídicos, as jurisprudências têm

desempenhado um papel importante na definição de diretrizes legais relacionadas à herança digital e aos bens digitais.

Desse modo, fica a cargo de cada legislador a autorização judicial para a destinação dos bens digitais. Apesar de diferentes entendimentos dos legisladores, acerca da destinação do patrimônio digital, salientamos como a ciência do direito tem se adaptado as transformações, bem como necessidades de uma sociedade cada vez mais digital.

Vejamos, agora, um pouco de como o assunto tem sido tratado fora do Brasil:

- Caso Facebook vs. Powertech: Em 2015, a justiça alemã decidiu que os pais de uma adolescente falecida tinham direito a acessar a conta de usuário do Facebook da filha falecida como herdeiros legais. A decisão reconheceu a importância dos bens digitais para o processo de luto e estabeleceu um precedente para casos similares.
- Caso Yahoo vs. Família Ajemian: Em 2009, a Suprema Corte de Massachusetts determinou que a família de um falecido tinha direito a acessar a conta de e-mail dele, considerando que os e-mails eram bens pessoais e não correspondências privadas. Essa decisão evidenciou a necessidade de equilíbrio entre a privacidade e os direitos sucessórios.
- Legislação Europeia de Proteção de Dados: O Regulamento Geral de Proteção de Dados da União Europeia, em vigor desde 2018, estabelece diretrizes para o tratamento de dados pessoais após a morte do titular, permitindo a nomeação de um representante para tomar decisões sobre os dados do falecido.

Sabemos que o direito à intimidade, à personalidade e à privacidade são o alicerce do Estado Democrático de Direito, assim, nasce a preocupação das normas do direito brasileiro acerca dos direitos da personalidade na herança digital.

Contudo, o Código Civil permite que, em algumas situações jurídicas, nas quais os Direito da Personalidade do falecido são violados, exista a possibilidade de uma tutela jurídica por parte dos familiares.

Assim, destaca Bittar (2015):

> Os Direito da Personalidade são classificados em: morais, quando relacionados com valores da pessoa f rente à sociedade, são eles a honra, o respeito, a imagem, a vida privada e outros; psíquicos, quando relacionados com a integridade psíquica, assim como são a intimidade, o segredo e as liberdades, em todas as suas expressões (de pensamento, de locomoção, de expressão, além de outros); e f ísicos, quando referentes à integridade corporal, assim como é o corpo humano e suas partes, o cadáver, a voz e outros.

Observa-se que em algumas jurisprudências sobre herança digital tem se analisado se os familiares ou herdeiros teriam direito ao acesso ou controle das contas e informações digitais de uma pessoa falecida. Contudo, algumas jurisdições têm adotado abordagens diversas que permitiriam o acesso aos dados digitais como parte da herança, enquanto outras têm sido mais restritivas.

Analisando o Enunciado 40 do Instituto Brasileiro de Direito de Família – IBDFAM (2021): "A herança digital pode integrar a sucessão do seu titular, ressalvadas as hipóteses envolvendo direitos personalíssimos, direitos de terceiros e disposições de última vontade em sentido contrário". Verifica-se que o enunciado serve de orientação com caráter doutrinário para os legisladores, portanto, a necessidade de adequação da legislação acerca do direito à herança dos ativos digitais pelos sucessores e dos direitos da personalidade do *de cujus*.

5. CONSIDERAÇÕES FINAIS

No Brasil, a temática da herança digital trouxe complexos desafios para as questões de herança e de sucessão. Atualmente, a resolução desses impasses tem sido resolvida por meio de interpretação dos tribunais com base no direito sucessório. No entanto, o direito dos herdeiros no que concerne à herança digital precisa passar a ser definido por uma legislação específica. Uma legislação que possua regramento apropriado a todas as características dos ativos digitais, bem como a separação dos ativos híbridos, existenciais e patrimoniais. Tal fato entende-se que os bens digitais patrimoniais e existenciais não devem ser definidos da mesma forma, haja vista que diferem em sua natureza. Atentamos para os ativos existenciais ou personalíssimos que devem receber uma regulamentação coerente com os direitos da personalidade, mesmo que com o advento das redes socias. Já os bens digitais de cunho patrimonial não hão o que se discutir, haja vista que a transmissão deveria ser automática aos herdeiros.

Consigna-se, por fim que o propósito desse artigo é demostrar a urgência de uma legislação específica para o tema. Uma vez legislada a herança digital pode auxiliar no planejamento sucessório, permitindo que as pessoas incluam os seus ativos digitais em seus testamentos e planejamentos sucessórios afim de garantir que os bens sejam transferidos conforme sua vontade, de maneira justa, protegendo a privacidade e os direitos do falecido.

REFERÊNCIAS

AUGUSTO, Naiara Czarnobai; OLIVEIRA, Rafael Nirbuhr Maia de. **A possibilidade jurídica da transmissão de bens digitais "causa mortis" em relação aos direitos personalíssimos do "*de cujus*"**. *In:* CONGRESSO IBEROAMERICANO DE INVESTIGADORES E DOCENTES DE DIREITO E INFORMÁTICA, 5., 2015, Santa

Maria, Rio Grande do Sul. Disponível em: https://www.ufsm.br/cursos/pos- graduacao/santa-maria/ppgd/congresso-direito-3a-edicao. Acesso em: 10 abr. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Nota Técnica nº 3/2023/CGF/ANPD**. Disponível em: https://www.in.gov.br/web/dou/-/resolucao- cd/anpd-n-3-de-25-de-janeiro-de-2023-460124477 Acesso em: 29 mar. 2024.

BITTAR, Carlos Alberto. **Os Direitos da Personalidade**. 8. ed. São Paulo: Saraiva, 2015.

BIZERRA, Yvana Barbosa. **Herança digital sob a** ótica **dos projetos legislativos brasileiros: uma análise do Direito Sucessório com o Direito da Personalidade do *de cujus***. 2021. Trabalho de Conclusão de Curso (Graduação em Direito) - Curso de Direito, Centro Universitário FG, Guanambi, Bahia. Disponível em: https://repositorio.animaeducacao.com.br/items/a547d1de-8897-4e7c-bbb6- 87bd7c9e635c. Acesso em: 10 abr. 2024.

BRASIL. Conselho da Justiça Federal. IX Jornada de Direito Civil. **Enunciado nº 687**. Disponível em: https://www.cjf.jus.br/enunciados/enunciado/1826. Acesso em: 10 abr. 2024.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília: Presidência da República, [2023]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 09 set. 2023.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília: Presidência a República, [2022]. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 09 set. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, [2018]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 09 set. 2023.

HERANÇA digital: Advogada explica como ficam os bens após a morte. **Migalhas**, [Brasil], 25 jul. 2023. Disponível em: https://www.migalhas.com.br/quentes/390556/heranca-digital-advogada-explica- como-ficam-os-bens--apos-a-morte. Acesso em: 09 set. 2023.

IBDFAM – Instituto Brasileiro de Direito de Família. **Enunciados IBDFAM**. Belo Horizonte, [2021]. Disponível em: https://ibdfam.org.br/publicacoes/enunciados. Acesso em: 10 abr. 2024.

LARA, Moisés Fagundes. **Herança Digital.** 1. ed. Porto Alegre: Clube dos Autores, 2016.

RIPPEL, Nathalia Gracinski. Herança digital: qual é o destino dos bens digitais do falecido no post morten. **Migalhas**, [Brasil], 1 nov. 2022. Disponível em: https://www.migalhas.com.br/depeso/376320/qual-e-o-destino--dos-bens-digitais-do- falecido-post-morten. Acesso em: 30 mar. 2024.

SOUZA, Devanildo de Amorim; SIQUEIRA, Luiz Eduardo Alves de. Desafios jurídicos da herança digital. **Consultor Jurídico**, [São Paulo], 23 ago. 2023. Disponível em: https://www.conjur.com.br/2023-ago-23/souza--siqueira-desafios-juridicos-heranca- digital/. Acesso em: 30 mar. 2024.

TARTUCE, Flavio. **Manual de direito civil: volume** único. 6. ed. São Paulo: Método, 2016. p. 1479.

XISTO, Ana Paula. **Herança digital: extensão e tutela da personalidade civil post mortem em harmonia com o direito** à **privacidade na rede**. 2018. Trabalho de Conclusão de Curso (Graduação em Direito) - Centro Universitário Toledo, Araçatuba, São Paulo. Disponível em: www.unitoledo.br/repositorio/handle/7574/2052. Acesso em: 10 abr. 2024.

ZAMPIER, Bruno. **Bens Digitais**. Indaiatuba: Foco, 2017. p. 74-112.

Capítulo 3

O Avanço Silencioso das Práticas Enganosas nas Relações de Consumo: A Proliferação das *Dark Patterns*

Mariana Palmeira

1. INTRODUÇÃO

É fato que a inovação tecnológica, aplicada ao campo do consumo, alimenta a discussão sobre a preponderância do *homo economicus*, ou seja, aquele que age para maximizar a utilidade de suas escolhas. Dessa maneira, interessa observar o avanço dos estudos sobre Economia Comportamental que propuseram a mudança de paradigma da racionalidade econômica para incluir a influência de variáveis mais complexas nos processos de decisão dos indivíduos em sociedade.

Também chamada de Behaviorismo, a Economia Comportamental pode ser definida, em poucas palavras, como "o estudo das influências cognitivas, sociais e emocionais observadas sobre o comportamento econômico das pessoas" (Samson, 2019).

Se, nas ciências econômicas, o impacto do Behaviorismo se deu no reconhecimento amplo de que os processos decisórios do homem não são ditados unicamente por sua racionalidade (Ribeiro & Domingues, 2018, p. 457), sua influência no marketing foi observada pela incorporação de técnicas propícias à exploração desta nova constatação. Trata-se do fenômeno chamado de "virada comportamental" (Nadler & McGuigan, 2018), que se apropria da gramática da Economia Comportamental e passa a direcionar esforços para explorar vulnerabilidades cognitivas e emocionais dos consumidores em seus processos de decisão de compra (p. 153).

O avanço tecnológico, combinado com a "virada comportamental" do marketing, sobretudo em ambiente digital, formou uma espécie de "tempestade perfeita" para o emprego de práticas que se aproximam mais da manipulação do comportamento de consumidores do que da influência sobre a preferência

por determinados produtos e serviços (Nadler & McGuigan, 2018, p. 152). Com ela, surgem os novos desafios para o Direito. O processo de decisão de compra do consumidor, desde os estímulos iniciais até a compra e o pós-compra, passa a ser diretamente impactado por essa combinação de fatores.

De especial importância são as tecnologias que viabilizam a apreensão de informações sobre o consumidor (ou consumidor em potencial) para que sejam usadas ao longo de todo o seu processo decisório. Grande parte desse uso é imperceptível aos olhos do público. Dito de outra maneira: a própria consciência do consumidor acerca de como os estímulos de compra são desenvolvidos e direcionados diminui. Dois fatores colaboram para essa invisibilidade: as chamadas *dark patterns* e a exploração de vieses comportamentais.

Neste artigo, parte-se da premissa de que a investigação no âmbito do Direito cumpre o papel de buscar oportunidades de emancipação para os grupos sociais (Gustin, 2020, p. 40), e leva-se em conta o cenário da incorporação da tecnologia no cotidiano do consumidor, muitas vezes de forma imperceptível, e da constante atualização das relações de consumo no que tange aos agentes econômicos e seus modelos de negócios, assim como no que se refere aos bens transacionados e aos recursos mobilizados pelo consumidor-usuário. Para isto, busca-se explorar o conceito de *dark patterns* inserido nas relações de consumo, e as primeiras implicações jurídicas. Divide-se em duas partes: primeiro apresenta-se o conceito em si. Em seguida aborda-se uma diferença fundamental para a análise das *dark patterns:* trata-se de influência ou de manipulação? Por fim, apresentam-se as considerações finais.

2. HISTÓRICO:

O termo *dark patterns* foi cunhado por Harry Brignull em 2009 e apresentado pela primeira vez em seu site darkpatterns.org, no qual descreveu um padrão de interfaces de usuário que se traduzem por "truques usados em websites e aplicativos que fazem você fazer coisas que você não faria, como comprar produtos ou assinar algum serviço" (Mathur et al., 2021, p. 3).

As *dark patterns* foram apontados em dois estudos contemporâneos sobre o poder das plataformas digitais. O primeiro é o relatório do governo norte-americano com foco na concorrência no mercado digital. O segundo é o relatório produzido pelo Stigler Center (2019), também voltado para plataformas digitais, que, de maneira mais ampla que o primeiro, estudou o impacto das plataformas digitais em quatro áreas relacionadas. São elas: economia; privacidade e segurança; imprensa; e funcionamento da democracia (Stigler Center, 2019, p. 7).

Ambos os relatórios indicam que os consumidores, de maneira geral, não têm condições de entender os aspectos negativos relacionados às suas atividades

em ambiente digital. Aos consumidores falta tempo, conhecimento e capacidade. E a tendência é que esse cenário se agrave à medida que as empresas se tornem mais sofisticadas no desenvolvimento de técnicas de manipulação (p. 12).

As *dark patterns* têm sido objeto de estudo da comunidade acadêmica desde 2009, quando Brignull cunhou o termo. A partir desse momento, é possível apontar pelo menos dois grupos de interesse. O primeiro deles se insere na área dos estudos de "Interação Humano-Computador" (IHC ou HIC em inglês), na qual, desde a década de 1980, são desenvolvidas pesquisas voltadas para as relações entre o ser humano e o computador (Mathur et al., 2021).

Trata-se de um campo inicialmente identificado com as ciências da computação, mas cujos horizontes se expandiram para abarcar investigações mais amplas. Temas como computação social e organizacional, acessibilidade para idosos, deficientes físicos e cognitivos, e um abrangente espectro de experiências e atividades humanas passaram a fazer parte da IHC.

Já o segundo grupo é formado pelos campos de interesse da psicologia, da economia, da filosofia e, mais recentemente, do direito. Referem-se a pesquisas que inicialmente se ocuparam em descrever o fenômeno a partir da perspectiva da modificação na arquitetura de escolha do usuário (Mathur et al., 2021, p. 12)[-]. Para tanto, definições foram estabelecidas, e diferentes formas de classificar as técnicas de *dark patterns* encontradas foram apresentadas (Bösch et al.. 2016; Gray et al., 2018). O resultado é uma sistematização acadêmica que é congruente, mas apresenta diferentes abordagens envolvendo tipos e atributos das *dark patterns*, bem como os efeitos provocados nos usuários (Mathur et al., 2021, p. 9).

Os estudos mais recentes passaram a se debruçar sobre a intensificação no uso das *dark patterns*, tendo como embasamento a taxonomia previamente desenvolvida. Em 2019, pesquisadores das universidades de Princeton e Chicago rastrearam mais de 11 mil websites de comércio eletrônico e revelaram a presença de *dark patterns* em 11% deles (Mathur et al., 2019). Na mesma linha, pesquisadores da universidade de Zurique identificaram *dark patterns* em 95% de um universo composto por 240 aplicativos selecionados da loja do Google (Google Play) (Geronimo et al., 2020, p. 1).

Questões ligadas à privacidade e à proteção de dados dos usuários também foram analisadas, como, por exemplo, estudos sobre *dark patterns* em avisos de cookies e em plataformas de consentimento (Utz et al., 2019). Destaca-se, em especial, a pesquisa realizada em 2016, na Universidade Ulm (Alemanha) (Bösch et al., 2016), pelo pioneirismo ao investigar o uso de técnicas para fazer com que os usuários entreguem suas informações pessoais de maneira contrária a seus próprios interesses. A partir de padrões de proteção de privacidade catalogados por Hoepman (2020), os autores desenvolveram uma classificação específica para *dark patterns* em privacidade.

Apesar de se tratar de um assunto relativamente novo, há a sensação familiar de se estar diante de algo que acontece há muito tempo no ambiente de negócios, o esforço de influenciar o consumidor. A ideia de "nome novo para prática antiga" permeia os trabalhos sobre *dark patterns*.

Porém, ela é atualmente analisada a partir de um novo contexto, que é o ambiente digital. É o que se extrai, por exemplo, da fala de Ryan Calo durante o workshop "Bringing Dark Patterns to Light" promovido pela "Federal Trade Commission" (FTC) em 2021:

> A ideia de que você pode manipular um ambiente para canalizar o comportamento tem uma longa linhagem. Pensamos em um exemplo da década de 1920, da ponte que Robert Moses supostamente fez para ter uma determinada altura de vão para que apenas pessoas ricas pudessem chegar à praia, porque, para o transporte público, era difícil passar sob uma ponte baixa.
> (...)
> Quando você passa de um ambiente físico para um ambiente digital, há mais aspectos do ambiente que você pode manipular (Estados Unidos..., 2021a, p. 3).

Em contexto digital, ganha outra proporção aquilo que já se encontrava normalizado aos olhos do consumidor no ambiente físico: por exemplo, técnicas como "preço psicológico", avisos de "últimas unidades" e "entrega das chaves". Nas palavras de Calo, "há mais aspectos para manipular" (Estados Unidos..., 2021a). Esses aspectos surgem de uma combinação de fatores que envolvem desde a captura da atenção do usuário, o tratamento dos dados pessoais daí advindos até a segmentação da audiência, a formação de perfis e o direcionamento de conteúdo individualizado.

No ambiente on-line, por exemplo, por meio dos testes A/B, as empresas têm a oportunidade de "refinar e aperfeiçoar as *dark patterns* que seus pares da era 'Mad Men' sequer podiam imaginar" (Luguri & Strahilevitz, 2021, p. 103). É possível testar e definir em tempo real, por exemplo, qual é a duração ideal de um cronômetro que mostra os minutos restantes de validade de uma oferta ou qual é o sombreado perfeito do tom de azul que atrai mais cliques, conforme afirmam Narayanan et al. (2020, p. 76) em revisão bibliográfica sobre *dark patterns*:

> Os testes A/B revelaram-se fundamentais para o desenvolvimento das "dark patterns" porque está longe de ser óbvio como traduzir um princípio abstrato como a "prova social" em um "nudge" concreto ("7 pessoas estão pesquisando sobre este hotel neste momento!"). Outro exemplo: Durante quanto tempo deve durar uma contagem decrescente mentirosa ("Este acordo expira em 15 minutos!" ... "14:59" ... "14:58" ...), para que o utilizador aja com urgência, mas não entre em pânico? Em tempo real, as experiências permitem aos designers encontrar as respostas com apenas algumas linhas de código.

Com efeito, volta-se para uma questão central no contexto das relações de consumo: o consumidor contemporâneo, inserido nesse ambiente digital, está sujeito apenas a técnicas agressivas (e toleradas) de marketing? Ou estaria ele diante de outro patamar de atuação por parte das empresas, no mesmo sentido afirmado por Shoshana Zuboff (2020, p. 23) acerca do capitalismo de vigilância, sem precedentes?

A investigação sobre o fenômeno das *dark patterns*, envolvendo suas definições e seus impactos junto ao consumidor, se apresenta valiosa nesse sentido; qual seja, trazer à tona uma faceta de um contexto maior, no qual todos estamos inseridos, chamado de capitalismo de vigilância.

Zuboff explica que, dentre os perigos que traz a ausência de precedentes, está a "normalização do anormal", aquilo que transforma o novo em uma continuação do passado, visto sob as lentes do passado e, portanto, dificilmente reconhecido como ameaça. Nesse sentido, importa trazer o tema à tona, retirá-lo do campo do marketing digital, em que esteve nos últimos anos.

Segundo Luguri & Strahilevitz (2021, p. 45), a diminuta publicação de resultados de pesquisas sobre a efetividade das *dark patterns*, em face do número crescente de websites e aplicativos que usam tais técnicas, revela tão somente a intenção de manter o assunto longe dos olhos dos reguladores e da opinião pública.

Em paralelo ao desenvolvimento das práticas de marketing digital, duas outras áreas também são consideradas precursoras das *dark patterns*: as pesquisas desenvolvidas em políticas públicas e *nudges*, e o "growth hacking". Thaler e Sunstein introduziram o termo *nudge*, que pode ser explicado por "iniciativas oriundas das esferas privadas e públicas que orientam as pessoas em determinadas direções, mas que ainda assim lhes permitem seguir o seu próprio caminho" (Mathur et al., 2021, p. 12).

A noção de autonomia inerente aos *nudges* foi reforçada pelo próprio Thaler (2018), ao afirmar que o aperfeiçoamento do ambiente de escolha (aquilo que ele chama de "arquitetura de escolha") faz com que as pessoas tomem melhores decisões (para elas), sem ter as opções limitadas. O crescimento das *dark patterns* é visto pelo autor como um desvio do que os *nudges* são, aquilo que passou a chamar de *sludge*: "atividades que estão essencialmente a empurrar para o mal." Dito de outra maneira: as técnicas usadas para induzir a boas escolhas a partir da perspectiva do usuário (*nudges*) passam a ser usadas em benefício do mercado empresarial, do lucro e do crescimento em primeiro plano.

A popularização e a profundidade da discussão nascente acerca das *dark patterns* é o que vai determinar como esse fenômeno será tratado no futuro. O esforço em ampliar o campo do conhecimento e apontar as implicações inicialmente para as relações de consumo, mas posteriormente para a sociedade, é o que marca o momento presente.

Recentemente, dois casos que envolvem a manipulação da audiência e o uso *dark patterns* vieram a público no Brasil. Um deles diz respeito aos recursos usados pela equipe da cantora Anitta (e seus fãs) para ajudar a música *Envolver* a chegar ao primeiro lugar do ranking global da plataforma de música Spotify. O outro caso se refere à empresa iFood e à contratação de agência de marketing digital com o objetivo de criar ações visando desmobilizar o movimento dos entregadores por melhores condições de trabalho (DiP et al., 2022).

No âmbito da pesquisa acadêmica, dois trabalhos recentes empreenderam esforços no sentido de apresentar um resumo da sistematização de *dark patterns* encontrada na literatura (Luguri & Strahilevitz, 2021, p. 53) e o conjunto de definições mais recorrentes (Mathur et al., 2021, p. 4). Em função de a produção acadêmica ser nova, as diferentes taxonomias desenvolvidas pelos autores – incluindo as autoridades de proteção ao consumidor e proteção de dados (a exemplo da CNIL e NCC), bem como órgãos governamentais (a exemplo de FTC e EDPB) – não permite detectar uniformidade no próprio conceito de *dark patterns* (Mathur et al. 2021, p. 7).

3. *DARK PATTERNS*: DA INFLUÊNCIA À MANIPULAÇÃO?

Efetivamente se pode afirmar que o interesse da comunidade jurídica sobre as *dark patterns* gira em torno de uma pergunta: Quais são os limites legais admissíveis? Dito de outra maneira: onde traçar a linha entre as práticas que são toleráveis e inseridas no contexto da livre iniciativa e do livre exercício da liberdade econômica e aquilo que deve ser considerado intolerável frente à proteção do consumidor e do titular de dados pessoais?

Antes, porém, do despertar de atenção de legisladores, reguladores e entidades de defesa do consumidor para os possíveis efeitos nefastos das *dark patterns*, técnicas assemelhadas permaneceram circunscritas à dinâmica própria da atividade do marketing –conforme já descrita no capítulo um do presente trabalho, marcada, durante todo o século XX, pelo objetivo de influenciar o consumidor na direção de produtos e serviços do fornecedor.

No entanto, a integração do marketing com a tecnologia, fenômeno conhecido por "martech" (Kotler et al., 2021, p. 11), ampliou o objetivo inicial para abarcar a predição. A capacidade de prever comportamento é peça-chave do chamado Marketing 5.0 , que passou a combinar a predição com a influência, como afirmam Kotler et al. (2021, p. 24)::

> O marketing preditivo é o processo de criar e utilizar a análise preditiva – em alguns casos com o uso de aprendizado de máquina para prever os resultados das atividades de marketing antes mesmo do lançamento. Essa primeira aplicação permite que as empresas visualizem qual será a reação do mercado, influenciando-a de maneira proativa.

Como consequência da inserção da predição no marketing, uma nova indústria surgiu e extrapolou as fronteiras das atividades comerciais. Trata-se da "indústria da influência", noção primeiramente desenvolvida pela organização Tactical Tech, que se dedica a estudar os efeitos da tecnologia na sociedade (Bentes, 2021). Portanto, parece natural que estratégias antes circunscritas ao marketing e, por isso, com menor potencial de atrair a atenção e o interesse da sociedade como um todo estão agora sob escrutínio. Nesse contexto também se inserem as *dark patterns*.

É fala recorrente entre os estudiosos de temas relacionados à influência a ideia de que não se está diante de grandes novidades, como ressalta a pesquisadora Anna Bentes (2021, p. 43-44):

> Claro que a busca por técnicas refinadas e efetivas para influenciar, conduzir e persuadir o comportamento humano, com ou sem auxílio de aparatos tecnológicos, já são desenvolvidas há muito tempo na história da humanidade. Porém, a particularidade dessa indústria é que a busca pelo potencial de prever e influenciar comportamentos torna-se, cada vez mais, um aspecto central do modelo de negócios que vem se formando nas primeiras décadas do século XXI através da internet e no mercado de dados e, por sua vez, que vem mudando a própria lógica do capitalismo.

Da mesma forma, os estudos sobre *dark patterns* fazem essa ressalva em relação ao ineditismo das técnicas, apontando como verdadeiramente novos o meio digital, a apreensão de dados pessoais e a escala proporcionada pela internet (Cf. Narayanan et al., 2020).

Um termo comumente vinculado à noção de influência que também remonta ao passado é a persuasão, característica integrante do discurso publicitário e inserida na própria definição da palavra publicidade: "comunicação não pessoal paga por um patrocinador identificado usando meios de comunicação de massa para persuadir ou influenciar uma audiência" (Moriarty et al., 2018, p. 578).

A associação entre as técnicas de persuasão e a publicidade retrocede ao início do século XX, com a aplicação de "modelos psicológicos para mobilizar o consumo das massas" (Bentes, 2021, p. 53). É célebre a obra *As armas da persuasão*, do psicólogo Robert Cialdini (2012), na qual ele apresenta os princípios da persuasão identificados após três anos de trabalho em áreas de marketing e publicidade de grandes empresas.

São eles: reciprocidade, compromisso e coerência, aprovação social, afeição, autoridade e escassez. Não causa surpresa a semelhança entre os princípios de Cialdini e as tipologias desenvolvidas para descrever as *dark patterns*. Neste contexto, cabe mencionar a recente manifestação de entidades de psicologia no sentido da apropriação dos saberes da respectiva área do conhecimento por

atores interessados na "manipulação de subjetividades de um modo inimaginável, até hoje, na história da humanidade" (Ferreira et al., 2021, p. 31).

Retomando a reflexão que tem permeado a recente produção jurídica sobre as *dark patterns* – qual seja, sua inserção lícita no âmbito das práticas comerciais –, observa-se a frequência com que a palavra "manipulação" aparece relacionada ao que se convencionou, no marketing e na publicidade, classificar como influência e persuasão.

Por isso, neste ponto, faz-se necessária uma breve digressão acerca de três termos que são frequentemente usados na literatura sobre as *dark patterns*. São eles: manipular, influenciar e persuadir. À exceção de manipular, os dois últimos também são usados na literatura sobre marketing. A depender do campo teórico, um termo prevalece sobre os demais, assim como diferentes significados podem ser atribuídos. Daí decorre a importância de colocar em evidência, ainda que brevemente, suas respectivas definições.

Não se pretende aqui adentrar em metodologias como análise de conteúdo ou análise de discurso, uma vez que não é este o objeto do presente trabalho. No entanto, a partir da pesquisa bibliográfica, foi possível observar que, ao lado dos verbos "influenciar e persuadir", bem como seus derivados "influência e persuasão", empregados com frequência no marketing, está a noção de "manipulação".

Segundo Robert Perloff (2017, p. 43), a manipulação é uma técnica de persuasão que ocorre quando os objetivos persuasivos não são revelados. A intenção é enganar o destinatário. Já de acordo com o Dicionário Michaelis, manipular apresenta seis significados, dos quais dois interessam à presente discussão: quais sejam, "Influenciar ou controlar um ou mais indivíduos de maneira ilegítima e de acordo com os próprios interesses; sugestionar" e "Provocar o falseamento da realidade; adulterar, falsear" (Manipular, 2022).

Importa ressaltar que, no primeiro significado, há a indicação do organizador da obra de se tratar de linguagem figurada: ou seja, aquela que aumenta a expressividade de um discurso, que pretende dar significados mais amplos e não literais. Destaca-se, nas duas definições, a associação do termo manipular a noções juridicamente proibidas: ilegitimidade e adulteração.

Já para a palavra influenciar, a mesma fonte trabalha com a noção do exercício de ascendência ou de sugestionamento sobre algo ou alguém. Interessa observar que a publicidade feita em ambiente digital ampliou o número de agentes usados para endossar produtos e serviços. São os chamados influenciadores digitais, que ganharam destaque e projeção comercial na internet pelo potencial que têm de afetar a opinião, o comportamento e a decisão de compra de seus públicos.

A relação de confiança com a audiência é o grande atributo dos influenciadores, o que faz do chamado Marketing de Influência um espaço propício

para práticas enganosas, como a não identificação de promoção de conteúdo publicitário. O movimento não passou despercebido pelas autoridades de proteção do consumidor e pelos órgãos de autorregulamentação publicitária de diversos países. No Brasil, o Conselho Nacional de Autorregulamentação Publicitária (CONAR) lançou um guia específico que determina as regras para o conteúdo comercial produzido pelos influenciadores (CONAR, 2021).

Por fim, a noção de persuadir é explicada por meios de palavras que remetem à ideia do convencimento, no sentido de levar alguém a tomar uma decisão, a acreditar em algo ou a mudar de ideia. Merece destaque a noção de que a autopersuasão é considerada a chave para o sucesso da influência. De acordo com Perloff (2017, p. 25), um dos grandes mitos sobre a persuasão é que as pessoas são convencidas a fazer aquilo que não desejam. Na visão do autor, a pessoa toma a decisão com base em argumentos persuasivos, mas inserida em ambientes de livre escolha.

Em uma visão mais crítica que a de Perloff, pensando a partir da perspectiva do anunciante, a ideia de autoconvencimento é a melhor possível, pois o consumidor não se dá conta da persuasão exercida sobre ele: "Todos se tornam agentes de persuasão. O segredo da persuasão é fazer a pessoa induzir a si mesma" (The Persuaders, 2004) Nessa mesma linha, Carissa Véliz (2020, p. 31) afirma que as grandes empresas de tecnologia investem justamente na característica manipulativa do *soft power*, o que transforma o usuário em cúmplice da própria manipulação exercida sobre ele.

4. CONSIDERAÇÕES FINAIS:

Em conclusão inicial sobre as acepções de manipulação, influência e persuasão aqui expostas, é possível extrair preliminarmente o sentido negativo e juridicamente condenável que o ato de manipular denota: seja em uma definição literal, que se associa ao falseamento da realidade ou à adulteração, seja em linguagem figurada, quando relativa à ilegitimidade da influência. Lembra-se, ainda, da intenção de enganar associada à palavra manipulação: "manobra feita às ocultas com o intuito de falsear a realidade" (Manipulação, 2022).

Importa ter em mente os diferentes significados atribuídos a cada um dos termos, pois a opção pela descrição de determinada prática como manipulativa, em detrimento de influência ou persuasão, aponta para a sua respectiva ilicitude. Porém, ressalta-se que estabelecer os limites entre influenciar e manipular o consumidor apresenta duas perspectivas distintas no que tange ao presente trabalho. A primeira delas se revela relevante na medida em que se assume (ou não) que a manipulação se insere em práticas abusivas, portanto vedadas pela legislação consumerista pátria.

De outra forma, em uma segunda perspectiva, a definição de limites e diferenças entre manipulação e influência deixa de ser significativa uma vez que o uso de *dark patterns*, ainda que entendido como circunscrito à legítima esfera da influência característica da atividade do marketing, enseja proteção diferenciada do consumidor.

Os padrões enganosos de design, sinônimo para *dark patterns*, somados a outras práticas de marketing em ambiente digital que serão exploradas mais adiante, são por si só suficientes para mudar a condição do consumidor. Além de vulnerável, ele passa também a ser hipossuficiente, pois dificilmente é capaz de compreender a arquitetura digital à qual está submetido.

A hipossuficiência se faz (oni)presente diante das práticas enganosas cada vez mais sofisticadas e imperceptíveis aos olhos do consumidor. Aquilo que é marca individual, que indica a debilidade processual e, em decorrência, autoriza a inversão do ônus da prova pelo magistrado se converte em marca universal. Resta impossível a realização de uma tutela jurídica justa enquanto a inversão do ônus da prova não estiver presente como regra no contexto das relações consumeristas travadas em ambiente digital.

Dito de outra maneira, a mera existência e utilização de *dark patterns*, independentemente do seu enquadramento legal, acaba por reforçar a hipótese de hipossuficiência do consumidor no mercado digital.

Os limites legais que foram postos sobre as relações de consumo remontam, no Brasil, ao Código de Defesa do Consumidor, diploma legal constituído antes da explosão da internet comercial, do e-commerce, da digitalização, das incontáveis possibilidades de uso dos dados pessoais. Da mesma forma, a atividade publicitária é fiscalizada majoritariamente com base na autorregulação proveniente do Código de Autorregulamentação Publicitária (CONAR). Seu conjunto de regras também carece de ferramentas para lidar com a nova escala que as *dark patterns* representam em termos de influência do consumidor.

O sempre complicado exercício jurídico-regulatório de promover o equilíbrio entre inovação, desenvolvimento econômico e proteção do consumidor se torna ainda mais instigante. Com o objetivo de compreender como as *dark patterns* representam novos desafios à proteção do consumidor, passa-se à apresentação sobre como o tema vem sendo tratado na literatura jurídica. A necessidade de compreensão e análise desses conceitos e da forma como vêm sendo aplicados às relações de consumo se faz imperiosa no bojo do presente trabalho.

REFERÊNCIAS

BENTES, A. A indústria da influência e a gestão algorítmica da atenção. In: FERREIRA, M.; BOCK, A.; GONÇALVES, M. G. M. **Estamos sob ataque!**: tecnologias de comunicação na disputa das subjetividades. São Paulo: Instituto Silvia Lane, 2021. p. 42-59.

BÖSCH, C. et al. Tales from the Dark Side: privacy dark strategies and privacy dark patterns. **Proceedings On Privacy Enhancing Technologies**, [S.L.], v. 2016, n. 4, p. 237-254, 14 jul. 2016.

BRIGNULL, H. Dark Patterns: dirty tricks designers use to make people do stuff. **90 Percent of Everything**, Nottingham, 8 jul. 2010. Disponível em: < https://90percentofeverything.com/2010/07/08/dark-patterns-dirty--tricks-designers-use-to-make-people-do-stuff/>. Acesso em 22 mar. 2022.

CALO, R.; ROSENBLAT, A. The Taking Economy: uber, information, and power. **Columbia Law Review**, [S.L.], v. 117, p. 1623-1690, 2017. Elsevier BV. http://dx.doi.org/10.2139/ssrn.2929643.

FERREIRA, M.; BOCK, A. GONÇALVES, M. Graça Marchina. **Estamos sob ataque!**: tecnologias de comunicação na disputa das subjetividades. São Paulo: Instituto Silvia Lane, 2021.

FTC Complaint: Ending an Amazon Prime Membership Is a Deceptive, Unlawful Ordeal. Public Citizenship, 14 jan. 2021. Disponível em: <https://www.citizen.org/news/ftc-complaint-ending-an-amazon-prime-membership--is-a-deceptive-unlawful-ordeal/>. Acesso em 22 mar. 2022.

GUSTIN, M. B. S. et al. **(Re)pensando a pesquisa jurídica**: teoria e prática. 5. ed. São Paulo: Almedina, 2020.

KOTLER, P.; ARMSTRONG, G. **Princípios de Marketing**. 15. ed. São Paulo: Pearson Education do Brasil, 2014.

_____.; KARTAJAYA, H.; SETIAWAN, I. **Marketing 5.0**: tecnologia para a humanidade. Rio de Janeiro: Sextante, 2021.

LUGURI, J.; STRAHILEVITZ, L. J. Shining a Light on Dark Patterns. **Journal Of Legal Analysis**, [S.L.], v. 13, n. 1, p. 43-109, 1 jan. 2021. Oxford University Press (OUP). http://dx.doi.org/10.1093/jla/laaa006. P. 105 –106.

MATHUR, A.; KSHIRSAGAR, M.; MAYER, J. What Makes a Dark Pattern... Dark? **Proceedings Of The 2021 Chi Conference On Human Factors In Computing Systems**, [S.L.], p. 1-27, 6 maio 2021. ACM. http://dx.doi.org/10.1145/3411764.3445610.

MORIARTY, S. et al. **Advertising & IMC**: principles & pratice. 11. ed. New York: Pearson, 2018.

NADLER, A.; MCGUIGAN, L. An impulse to exploit: the behavioral turn in data-driven marketing, **Critical Studies in Media Communication**, vol. 35. n. 2, p.151-165, 2018.

NARAYANAN, A. et al. Dark Patterns Past, Present, and Future: the evolution of tricky user interfaces. **Acm Queue.** [S.I], p. 67-91. mar. 2020.

PERLOFF, R. M. **The Dynamics of Persuasion**: communications and attitudes in the 21st century. 6. ed. New York: Routledge, 2017.

RIBEIRO, M.; DOMINGUES, V. Economia Comportamental e direito: a racionalidade em mudança. **Revista Brasileira de Políticas Públicas**. vol. 8. n. 2. 2018. p. 456-471.

SAMSON, A. Introdução à economia comportamental e experimental. In: ÁVILA, F. et al. **Guia de Economia Comportamental e Experimental**. 2. ed. São Paulo: Economiacomportamental.Org, 2019. Cap. 1. p. 26-59.

VÉLIZ, C. **Privacy is power**: why and how you should take back control of your data. [S.I]: Bantam Press, 2020.

ZUBOFF, S. **A Era do capitalismo de vigilância**. Rio de Janeiro: Intrínseca, 2020.

Capítulo 4

Os Contratos Inteligentes no Agronegócio: Como a Tecnologia está Transformando as Relações Comerciais no setor Agrícola

Marina Pantoja
Pollyanna Kruger

INTRODUÇÃO

A revolução digital trouxe diversas inovações para o agronegócio, com tecnologias emergentes redefinindo práticas tradicionais. Entre essas inovações, os contratos inteligentes, ou *smart contracts,* destacam-se por sua capacidade de automatizar, simplificar e tornar mais seguras as transações comerciais no setor agrícola. Assim, os contratos inteligentes estão transformando as relações comerciais no setor agrícola brasileiro, melhorando sensivelmente a dinâmica comercial no nosso agronegócio que, por sua vez, por se tornar cada vez mais rico, exige inovações capazes de responder às demandas diárias dos profissionais que precisam otimizar o tempo sem, contudo, abrir mão da qualidade e segurança jurídica exigidos para negociações que envolvem contratos de grande monta.

A aplicação dos contratos inteligentes no agronegócio traz maior eficiência, transparência e segurança das transações comerciais, mas também apresenta desafios em sua implementação para os quais os profissionais atuantes no setor precisam estar preparados[1].

Os contratos inteligentes, ou *smart contracts*, são programas de computador que executam automaticamente os termos e condições de um contrato quando as condições pré-definidas são atendidas pelas partes. Esses contratos são autoexecutáveis, eliminando a necessidade de intermediários para a verificação e execução das cláusulas contratuais.

---

[1] LIN, Qijun; WANG, Huaizhen; PEI, Xiaofu; et al. Food Safety Traceability System Based on Blockchain and EPCIS. IEEE, v. 7, 2019.

Frequentemente os contratos inteligentes são implementados em plataformas de *blockchain*, que são registros digitais descentralizados e imutáveis. A *blockchain* fornece a infraestrutura necessária para que os contratos inteligentes sejam seguros, instintivos e transparentes.

Por se tratar de uma forma de negociação e contratação não tradicional, a pergunta frequente é qual seria, então, a forma base para elaboração, controle de cumprimento e validação dos *smart contracts*.

A blockchain, tecnologia frequentemente utilizada nos smart contracts, contém um conjunto de transações ou dados que são validados e ligados ao bloco anterior através de criptografia. O funcionamento dos blocos consiste em conter transações ou registros, formando uma cadeia interligada de informações criptografadas. A blockchain é mantida por uma rede global de computadores, chamados nós. Cada nó possui uma cópia completa do livro-razão. As transações são validadas por todos os nós da rede através de um processo de consenso, com métodos como Proof of Work (PoW) e Proof of Stake (PoS). Uma vez que um bloco é adicionado, ele não poderá ser alterado, garantindo segurança contra fraudes e manipulações, trazendo a segurança jurídica necessária para a assinatura digital do contrato.

Entre as características principais da blockchain, estão a transparência, onde todas as transações são visíveis para todos os participantes da rede, e a segurança, onde a criptografia e a descentralização garantem a rede contra ataques. Não há, entretanto, uma autoridade central, como se costuma ter no caso de contratos assinados em cartórios e conferidos por tabeliães. Os nós, nesse caso, colaboram para validar e registrar transações, garantindo a descentralização. As transações registradas não podem ser alteradas, proporcionando um histórico confiável e imutável.

As aplicações da blockchain incluem criptomoedas, facilitando transações financeiras seguras e descentralizadas, como com Bitcoin e Ethereum. Também há contratos inteligentes autoexecutáveis, ou seja, sem atuação de intermediários, quando as condições pré-definidas são atendidas. Na *supply chain*[2], a blockchain permite monitoramento transparente e rastreável da cadeia de suprimentos, garantindo a autenticidade dos produtos[3]. Na votação eletrônica, por exemplo, a segurança e transparência da blockchain a tornam ideal para sistemas de votação, prevenindo fraudes. Para registros médicos, a

---

2 Termo em inglês que define todas as etapas dos processos aos quais os produtos são submetidos. Em outros termos, ilustra o caminho que cada mercadoria faz desde a saída da matéria-prima das fazendas e centros produtores, até a etapa de consumo final. Ela engloba todas as operações que envolvem a produção, logística e distribuição.

3 DOS SANTOS, Ricardo Borges; TORRISI, Nunzio Marco; PANTONI, Rodrigo Palucci. Third Party Certification of Agri-Food Supply Chain Using Smart Contracts and Blockchain Tokens. Sensors, v. 21, p. 5307, 2021.

blockchain armazena dados de forma segura e acessível, garantindo a privacidade dos pacientes e a segurança jurídica de clínicas, hospitais e profissionais autônimos que lidam com informações sensíveis.

As vantagens da blockchain incluem transparência e confiança, onde a visibilidade total das transações aumenta a confiança. A segurança protege contra fraudes e ataques cibernéticos com criptografia avançada. A eficiência reduz a necessidade de intermediários e acelera a verificação e validação de transações. A descentralização elimina riscos de monopólio e corrupção ao não depender de uma autoridade central. E todos esses fatores contribuem para a otimização e modernização do agronegócio, mas também para os objetivos de desenvolvimento sustentável, contribuindo para a diminuição na emissão de gazes de efeito estufa e utilização desnecessária de papeis.

Por outro lado, ainda há desafios na utilização dos *smart contracts* através da plataforma blockchain. A capacidade limitada de processar grandes volumes de transações por segundo, por exemplo, é um desafio. O consumo de energia é uma preocupação, pois algoritmos de consenso, como o *Proof of Work* (algoritmo prova de trabalho, em português), ou simplesmente PoW, exigem o consumo de muita energia.

Além disso, a regulamentação incipiente dessa prática contratual ainda traz incertezas para alguns produtores, que acabam preferindo a utilização de métodos contratuais tradicionais, mais dispendiosos, com necessidade muitas vezes de mais de um intermediador para garantir o respeito às cláusulas, em razão da falta de segurança nas informações. Além disso, a implementação e manutenção da *blockchain* para garantia da execução dos *smart contracts* podem ser complexas, exigindo conhecimentos técnicos especializados.

O gerenciamento de contratos inteligentes através da tecnologia *blockchain* é uma proposta inovadora que oferece segurança, transparência e descentralização para registrar, verificar e validar transações. Suas aplicações vão além dos contratos inteligentes, abrangendo também as criptomoedas e outros mecanismos de trabalho e certificação de registros. Apesar dos desafios, a autoexecutoriedade desse tipo de contrato, o controle independente e os aspectos econômicos e não poluentes representam uma importante solução para o agronegócio brasileiro.

A REVOLUÇÃO DOS CONTRATOS INTELIGENTES AUTOEXECUTÁVEIS NO AGRONEGÓCIO BRASILEIRO

Os contratos inteligentes baseados em *blockchain* representam uma tecnologia inovadora capaz de disseminar informações, verificar, negociar automaticamente, executar e fazer cumprir os termos de um acordo intrapartes em

um ambiente de *blockchain*. Em comparação com os contratos tradicionais, os contratos inteligentes destacam-se por seu baixo custo, elevado grau de automação, alta eficiência e robusta segurança[4]. Além disso, esses contratos possuem a capacidade de autocensura e autoexecutoriedade, características impensáveis nos contratos tradicionais.

No agronegócio brasileiro, a implementação dos contratos inteligentes inicia com a integração das partes interessadas dentro da cadeia de suprimentos. Posteriormente, esses contratos são customizados conforme as necessidades específicas. Até então, nada de realmente diferente do que se costuma acompanhar nas técnicas tradicionais de negociação contratual. Elemento vontade, partes interessadas em pleno gozo de suas capacidades civil e mental, pleno conhecimento dos fatos, objeto lícito, possível, identificado ou identificável.

A transferência de todas essas informações para a plataforma *blockchain*, no entanto, e diferentemente do que existia no método tradicional, é capaz de superar as barreiras de interação de dados na cadeia de suprimentos, resolvendo problemas fundamentais como a falsificação de dados e a dificuldade de peticionamento.

Com a automação avançada proporcionada pelos contratos inteligentes, é possível exercer um controle mais rigoroso sobre a qualidade na indústria agrícola, assim como no fornecimento de matérias primas e controle de maquinário e transportes[5]. Dessa forma, a aplicação de contratos inteligentes oferecem avanços significativos no processo de digitalização do setor.

A mercantilização de informações, no entanto, é um passo crucial que o agronegócio brasileiro deve enfrentar durante seu processo de digitalização. Contratos inteligentes em têm o potencial de resolver problemas como confirmação de dados, supervisão confiável e rastreabilidade, beneficiando empresas, autoridades reguladoras e consumidores , de um lado, mas de outro oferece também os riscos inerentes à exposição de dados em nuvens, e esse é um dos principais motivos pelos quais os setores devem buscar consulta com profissionais qualificados e de confiança.

Estudos preliminares sobre a aplicação de contratos inteligentes em blockchain mostram que, inicialmente, esses contratos surgiram como programas embutidos no código central de *blockchains*, como o Bitcoin. Com o avanço das pesquisas, outras várias formas de elaboração de contratos inteligentes se desenvolveram.

---

4 WANG, Lu; XU, Longqin; ZHENG, Zhiying; et al. Smart Contract-Based Agricultural Food Supply Chain Traceability. IEEE, v. 9, 2021.

5 ALVES, E.; SOUZA, G.; SANTANA, C. Pobreza e sustentabilidade. Revista de Política Agrícola, v. 25, n. 4, p. 63-81, 2016. BRASIL. Ministério da Agricultura, Pecuária e Abastecimento. Sisbov. Brasília, DF, 2017.

Como um motor poderoso para a transformação digital da indústria do agronegócio, os contratos inteligentes em *blockchain* têm uma definição única e desempenham um papel específico. Sua aplicação, no entanto, ainda está em fase de descoberta e conquista do mercado. Com a crescente evolução dessa tecnologia, torna-se difícil para os profissionais assimilarem o conhecimento essencial e as últimas novidades do campo.

Ainda com as desvantagens, os benefícios da adoção dos *smart contracts* contam com uma vasta lista de tópicos. A imutabilidade é o primeiro, uma vez que um contrato inteligente é registrado na *blockchain*, ele não pode ser alterado. Isso garante a integridade e a segurança das transações.

A execução dos contratos inteligentes não depende de uma autoridade central. Em vez disso, eles são validados pela rede de nós (computadores) que integram aa blockchain e todas as partes envolvidas em um contrato inteligente podem verificar as condições e a execução do contrato, que estão públicas e de fácil acesso.

Dentre as desvantagens atuais, a criação de contratos inteligentes requer conhecimentos técnicos avançados em programação e *blockchain*; a falta de um marco regulatório claro pode dificultar a aplicação legal dos contratos inteligentes em alguns contextos, além de trazer falta de confiança às partes, que desconhecem as garantias desse tipo de contrato.

A implementação inicial de contratos inteligentes pode ter custo elevado, devido ao desenvolvimento e integração com sistemas preexistentes[6].

Por outro lado, contratos inteligentes podem automatizar pagamentos entre compradores e vendedores de produtos agrícolas. Quando o produto é entregue e verificado, o pagamento é automaticamente liberado para o vendedor, reduzindo atrasos e disputas. Em transações de financiamento agrícola, os contratos inteligentes podem liberar fundos automaticamente com base em condições pré-estabelecidas, como a entrega de insumos ou o cumprimento de marcos de produção.

RASTREABILIDADE E TRANSPARÊNCIA

Contratos inteligentes podem rastrear produtos desde a origem até o consumidor final, registrando todas as etapas da cadeia de suprimentos na blockchain. Isso garante que todas as partes envolvidas tenham acesso a um histórico completo e imutável do produto. A atualização automática de inventário e a reordenação de insumos podem ser gerenciadas por esses contratos, garantindo que os estoques sejam mantidos de forma eficiente.

---

6 PINCHEIRA, Miguel; VECCHIO, Massimo; GIAFFREDA, Raffaele; et al. Cost-effective IoT devices as trustworthy data sources for a blockchain-based water management system in precision agriculture. Computers and Electronics in Agriculture, v. 180, 2021.

REDUÇÃO DE INTERMEDIÁRIOS

Ao eliminar a necessidade de intermediários para a verificação e execução de contratos, os contratos inteligentes reduzem os custos operacionais e aumentam a eficiência das transações. Isso pode ser particularmente benéfico para pequenos agricultores, que frequentemente enfrentam altos custos de transação. Ou seja, a adoção de contratos inteligentes pode ter um custo elevado incialmente, mas, uma vez implementado, tem o condão de reduzir os custos.

AUMENTO DA CONFIANÇA ENTRE AS PARTES

A execução automática e imparcial dos contratos aumenta a confiança entre as partes envolvidas. Todas as transações e condições são registradas de forma imutável na *blockchain*, proporcionando um histórico transparente e auditável. Se, incialmente, as parte se sentem inseguras por falta de conhecimento da tecnologia, posteriormente essa insegurança some com as garantias prestadas pelas informações trazidas pela tecnologia.

COMPLIANCE

Contratos inteligentes podem monitorar e registrar práticas agrícolas sustentáveis, assegurando que os produtores estejam em conformidade com normas ambientais[7]. Em casos de perdas devido a eventos climáticos ou pragas, pode haver verificação automática de dados de sensores ou imagens de satélite, com a consequente liberação de pagamentos de seguro aos agricultores sem a necessidade de processos judiciais burocráticos e demorados.

Agricultores e empresas podem ser resistentes à mudança e à adoção de novas tecnologias, especialmente se não estiverem familiarizados com elas. A falta de entendimento e confiança na tecnologia *blockchain* pode dificultar a aceitação dos contratos inteligentes, as o fato é que, cedo ou tarde, a adoção de tecnologias nos processos judiciais e extrajudiciais, na regulamentação administrativa e na prestação de serviços tomará espaço de forma irremediável. As vantagens são incontáveis, e as desvantagens, de outro lado, são perfeitamente contornáveis em nome de um sistema jurídico mais autônomo e confiável.

CONCLUSÃO

A aplicação de contratos inteligentes no agronegócio tem o potencial de revolucionar o setor, trazendo maior eficiência, transparência e segurança.

---

7 YANG, Xinting; LI, Mengqi; YU, Huajing; et al. A Trusted Blockchain-Based Traceability System for Fruit and Vegetable Agricultural Products. IEEE, v. 9, 2021.

No entanto, a adoção generalizada dessa tecnologia depende da superação de desafios tecnológicos, legais e culturais. A previsão é que, com o avanço tecnológico e a adaptação do setor, os contratos inteligentes se tornem uma prática comum, transformando profundamente as relações comerciais no agronegócio e trazendo uma nova forma de atuação para o setor público, advogados, consultores, produtores rurais e consumidores de produtos de origem agrícola.

REFERENCIAS

ALDRIGHI, D. M. Uma avaliação das contribuições de Stiglitz à teoria dos mercados financeiros. Revista de Economia Política, v. 26, p. 137-57, 2006.

ALVES, E.; SOUZA, G.; SANTANA, C. Pobreza e sustentabilidade. Revista de Política Agrícola, v. 25, n. 4, p. 63-81, 2016. BRASIL. Ministério da Agricultura, Pecuária e Abastecimento. Sisbov. Brasília, DF, 2017.

ANTONUCCI, Francesca; FIGORILLI, Simone; COSTA, Corrado; et al. A review on blockchain applications in the agri-food sector. JSFA, v. 99, p. 6129, 2019.

CHRISTIDIS, Konstantinos; DEVETSIKIOTIS, Michael. Blockchains and Smart Contracts for the Internet of Things. IEEE, v. 4, p. 2292, 2016.

COCCO, Luisanna; MANNARO, Katiuscia; TONELLI, Roberto; et al. A Blockchain-Based Traceability System in Agri-Food SME: Case Study of a Traditional Bakery. IEEE, v. 96, p. 2899, 2021.

DOS SANTOS, Ricardo Borges; TORRISI, Nunzio Marco; PANTONI, Rodrigo Palucci. Third Party Certification of Agri-Food Supply Chain Using Smart Contracts and Blockchain Tokens. Sensors, v. 21, p. 5307, 2021.

FERDOUSI, Tanvir; GRUENBACHER, Don; SCOGLIO, Caterina M. A Permissioned Distributed Ledger for the US Beef Cattle Supply Chain. IEEE, v. 8, p. 4833, 2020.

HANG, Lei; ULLAH, Israr; KIM, Do-Hyeun. A secure fish farm platform based on blockchain for agriculture data integrity. Computers and Electronics in Agriculture, v. 170, p. 05251, 2020.

JAMIL, Faisal; IBRAHIM, Muhammad; ULLAH, Israr; et al. Optimal smart contract for autonomous greenhouse environment based on IoT blockchain network in agriculture. Computers and Electronics in Agriculture, v. 192, p. 06573, 2022.

KHAN, Prince Waqas; BYUN, Yung-Cheol; PARK, Namje. IoT-Blockchain Enabled Optimized Provenance System for Food Industry 4.0 Using Advanced Deep Learning. Sensors, v. 20, p. 2990, 2020.

LIN, Qijun; WANG, Huaizhen; PEI, Xiaofu; et al. Food Safety Traceability System Based on Blockchain and EPCIS. IEEE, v. 7, p. 20698, 2019.

LUO, Qiqi; LIAO, Ruizhi; LI, Jiawei; et al. Blockchain Enabled Credibility Applications: Extant Issues, Frameworks and Cases. IEEE, v. 10, p. 45759, 2022.

MARCHESI, Lodovica; MANNARO, Katiuscia; MARCHESI, Michele; et al. Automatic Generation of Ethereum-Based Smart Contracts for Agri-Food Traceability System. IEEE, v. 10, p. 50363, 2022.

PINCHEIRA, Miguel; VECCHIO, Massimo; GIAFFREDA, Raffaele; et al. Cost-effective IoT devices as trustworthy data sources for a blockchain-based water management system in precision agriculture. Computers and Electronics in Agriculture, v. 180, p. 05889, 2021.

RAHMAN, Md. Abdur; RASHID, Md. Mamunur; HOSSAIN, M. Shamim; et al. Blockchain and IoT-Based Cognitive Edge Framework for Sharing Economy Services in a Smart City. IEEE, v. 7, p. 18611, 2019.

SALAH, Khaled; NIZAMUDDIN, Nishara; JAYARAMAN, Raja; et al. Blockchain-Based Soybean Traceability in Agricultural Supply Chain. IEEE, v. 7, p. 73295, 2019.

SHAHID, Affaf; ALMOGREN, Ahmad; JAVAID, Nadeem; et al. Blockchain-Based Agri-Food Supply Chain: A Complete Solution. IEEE, v. 8, p. 69230, 2020.

TAO, Qi; CUI, Xiaohui; HUANG, Xiaofang; et al. Food Safety Supervision System Based on Hierarchical Multi-Domain Blockchain Network. IEEE, v. 7, p. 51817, 2019.

WANG, Lu; XU, Longqin; ZHENG, Zhiying; et al. Smart Contract-Based Agricultural Food Supply Chain Traceability. IEEE, v. 9, p. 9296, 2021.

WANG, Shangping; LI, Dongyi; ZHANG, Yaling; et al. Smart Contract-Based Product Traceability System in the Supply Chain Scenario. IEEE, v. 7, p. 5122, 2019.

YANG, Haotian; XIONG, Shuming; FRIMPONG, Samuel Akwasi; et al. A Consortium Blockchain-Based Agricultural Machinery Scheduling System. Sensors, v. 20, p. 2643, 2020.

YANG, Xinting; LI, Mengqi; YU, Huajing; et al. A Trusted Blockchain-Based Traceability System for Fruit and Vegetable Agricultural Products. IEEE, v. 9, p. 36282, 2021.

YU, Bin; ZHAN, Ping; LEI, Ming; et al. Food Quality Monitoring System Based on Smart Contracts and Evaluation Models. IEEE, v. 8, p. 12479, 2020.

ZHANG, Lejun; ZHANG, Zhijie; WANG, Weizheng; et al. Research on a Covert Communication Model Realized by Using Smart Contracts in Blockchain Environment. Information Systems Journal, v. 16, p. 2822, 2022.

ZHANG, Xin; SUN, Pengcheng; XU, Jiping. Blockchain-Based Safety Management System for the Grain Supply Chain. IEEE, v. 8, p. 36398, 2020.

ATZORI, Marcella. Blockchain technology and decentralized governance: Is the State still necessary? SSRN, 2015. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713. Acesso em: 16 out. 2018.

AUNG, Y. N.; TANTIDHAM, T. Review of Ethereum: Smart home case study. In: Information Technology (INCIT), 2017 2nd International Conference on. IEEE, 2017. p. 1-4.

BORRERO, Juan D. Sistema de rastreabilidade da cadeia de suprimento agroalimentar para cooperativas de frutas e hortaliças baseado na tecnologia Blockchain. CIRIEC-España, Revista de Economía Pública, Social e Cooperativa, n. 95, p. 71-94, 2019.

BUTERIN, V.; et al. A next-generation smart contract and decentralized application platform. White Paper, 2014.

DENNY, D. M. T.; PAULO, R. F.; DE CASTRO, D. Blockchain and Agenda 2030. Braz. J. Pub. Pol'y, v. 7, p. 122, 2017.

GALVEZ, Juan F.; MEJUTO, J. C.; SIMAL-GANDARA, J. Future challenges on the use of blockchain for food traceability analysis. TrAC Trends in Analytical Chemistry, 2018.

LENG, K.; et al. Research on agricultural supply chain system with double chain architecture based on blockchain technology. Future Generation Computer Systems, 2018.

NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. Japan, 2008.

SZABO, N. Smart Contract. Online, 1994. Disponível em: https://bit.ly/2rLG2Nr. Acesso em: 16 out. 2018.

WRIGHT, A.; DE FILIPPI, P. Decentralized blockchain technology and the rise of lex cryptographia. SSRN, 2015.

YANO, Inácio Henrique; et al. Modelo de rastreamento bovino via Smart Contracts com tecnologia Blockchain. Embrapa Informática Agropecuária-Comunicado Técnico (INFOTECA-E), 2018.

ZAGONEL, T. R.; et al. BLOCKCHAIN E SMART CONTRACTS NO AGRONEGÓCIO. In: VII Simpósio da Ciência do Agronegócio, nº 7, 2019. Porto Alegre, Rio Grande do Sul, Brasil. Anais... Porto Alegre: Universidade Federal do Rio Grande do Sul, 2019. p. 47-56.

Capítulo 5
Uma Breve História do Phishing...

Cleber Soares
Deivison Franco
Joas Santos

Com o mundo evoluindo rapidamente, é desafiador acompanhar todas as novas tecnologias. Isso também significa que os crimes cometidos por meio de dispositivos tecnológicos têm características distintas dos crimes convencionais. O phishing, por exemplo, é uma forma de fraude tecnológica que envolve a obtenção fraudulenta de dados eletrônicos pela internet. Geralmente, é categorizado como peculato ou furto qualificado, podendo resultar em brechas de segurança e danos às empresas.

Neste artigo, vamos discutir o phishing e outras formas de fraude tecnológica, como Spear Phishing, Vishing, Phishing Offline, Dumpster Diving, Typosquatting, Phishing de QR Code, Pharming e Encurtadores de Link. Nosso objetivo é esclarecer e ajudar o público a entender as diferentes maneiras de ataques cibernéticos aos quais estão expostos, além de oferecer orientações sobre como prevenir e evitar esses ataques, tanto no ambiente corporativo quanto no pessoal.

A ORIGEM DO PHISHING

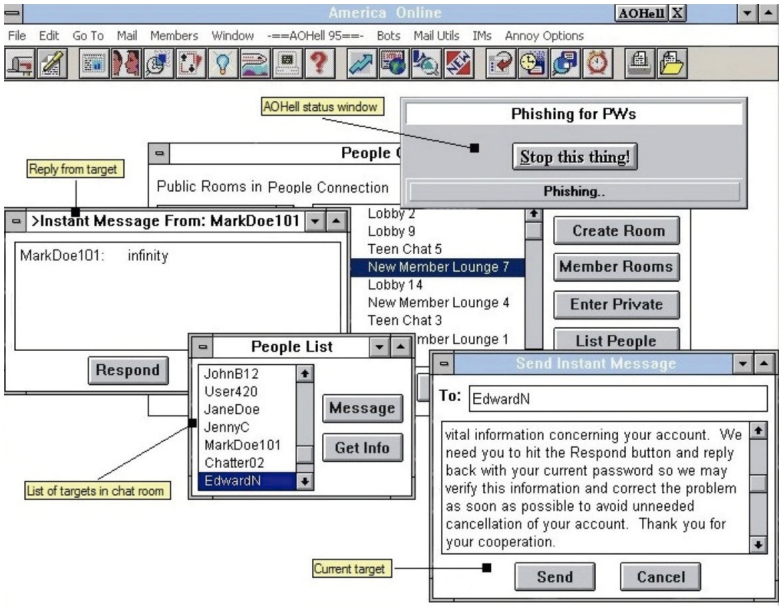
O termo "phishing" surgiu em 28 de janeiro de 1996, cerca de uma década após a fundação da AOL (America Online) em 1985. A AOL, que era o maior provedor de Internet do mundo naquela época, popularizou-se por distribuir disquetes e CDs promocionais que ofereciam horas de acesso gratuito à internet como estratégia de marketing. O phishing, uma técnica fraudulenta, foi identificado pela primeira vez quando funcionários da AOL tentaram obter credenciais de acesso à internet de maneira ilícita. Esse incidente destacou a necessidade de conscientização e segurança online, dando início à luta contra essa modalidade de crime cibernético.

Em um fórum chamado “AOL for free?”, o usuário “mk590”, publicou o seguinte excerto:

> “O que acontece é que antigamente, podia-se fazer uma conta falsa na AOL, uma vez que se tivesse um gerador de cartões de crédito. Porém, a AOL foi esperta. Agora, após digitar-se os dados do cartão, é feita uma verificação com o respectivo banco. Alguém mais conhece outra maneira de adquirir uma conta que não seja através de Phishing?”

Na década de 1980, para se conectar à internet discada através do provedor AOL, os usuários precisavam se cadastrar utilizando um cartão de crédito. Os “crackers” aproveitaram essa situação criando um programa chamado AOHell, que gerava números de cartão de crédito aleatórios para abrir contas, pois a AOL não validava esses números inicialmente. Com o tempo, a AOL começou a validar os números de cartão em parceria com as operadoras de crédito, dificultando essa prática fraudulenta.

Figura 1
Programa AOHell, gerenciava credenciais da AOL e cartões de crédito



Os ataques de phishing podem ocorrer de diversas formas, sendo uma das mais tradicionais por meio de comunicação eletrônica. Essa prática crimi-

nosa vem crescendo a cada ano, com milhares de e-mails fraudulentos enviados diariamente. Esses e-mails contêm links que direcionam para sites falsos que se passam por legítimos ou anexos maliciosos, com o objetivo de obter ilegalmente informações confidenciais de empresas ou indivíduos. Essas campanhas podem ser muito lucrativas para os cibercriminosos, que visam explorar o "elo mais fraco" de uma organização: o usuário.

Os e-mails de phishing frequentemente fingem ser de instituições bancárias, solicitando que o destinatário clique em um link para uma atualização de segurança ou sincronização com um gerador de senhas (token). É importante destacar que nenhuma instituição bancária solicita esse tipo de ação por e-mail. Outra abordagem comum é se passar por instituições governamentais, enviando mensagens que contêm ameaças relacionadas a investigações ou problemas com a declaração de imposto de renda, pedindo que o destinatário clique em um link ou baixe um arquivo, sob pena de sérias consequências.

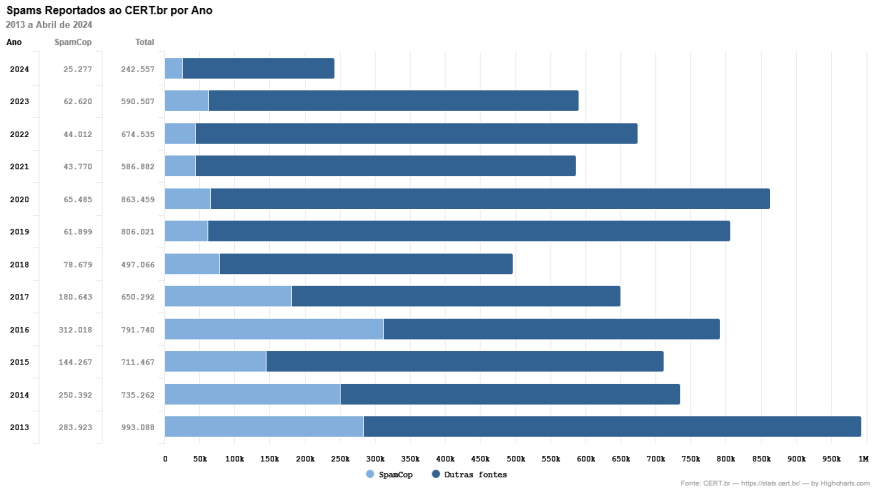
Alguns usuários são atraídos pela curiosidade, recebendo e-mails que parecem ser notas de compra, com a descrição de itens e um link para visualizar o relatório. Em outros casos, os criminosos forjam o remetente do e-mail para parecer um endereço confiável. Para identificar a autenticidade do remetente, é possível analisar o cabeçalho do e-mail, verificando o caminho percorrido desde o remetente até os servidores de e-mail do destinatário.

SPAM E PHISHING: O QUE TÊM EM COMUM?

A sigla "SPAM" corresponde a "Enviar e Publicar Anúncio em Massa". Fazendo uma analogia, seria como receber panfletos ou ver cartazes oferecendo produtos, mas no formato digital. Os responsáveis por essas ações, conhecidos como spammers, têm como objetivo principal enviar o maior número possível de e-mails indesejados para diversos usuários. Esses e-mails podem ser maliciosos ou simplesmente anúncios de produtos e serviços, muitas vezes prometendo vantagens excessivas e duvidosas.

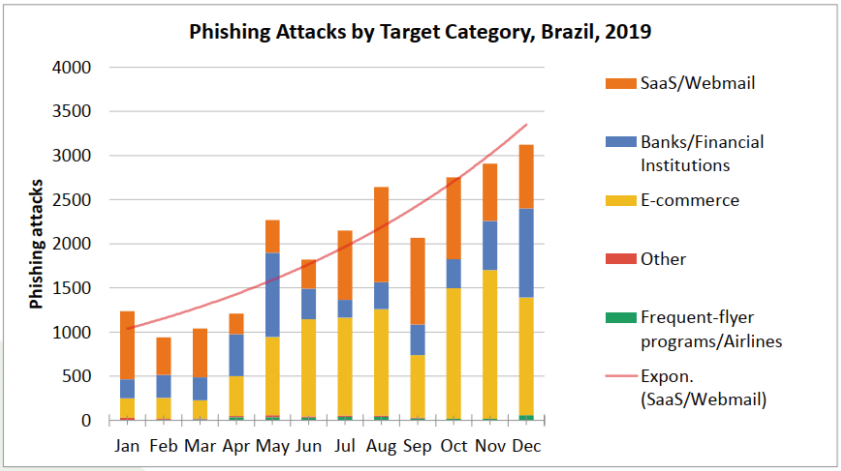
Muitos serviços de e-mail possuem proteções contra spam e oferecem ferramentas para que os usuários denunciem mensagens indesejadas. No entanto, de acordo com o Cert.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), que é mantido pelo NIC.br (Núcleo de Informação e Coordenação do Ponto BR), entre 2013 e 2024, foram reportados inúmeros e-mails indesejados, evidenciando a persistência desse problema.

Figura 2
Report Cert.br



O grupo APWG (Anti-Phishing Working Group) é uma organização que reúne instituições, empresas e parceiros globais afetados por ataques de phishing e outras técnicas de fraude online. Eles reportam incidentes e fornecem informações através do site http://www.apwg.org, além de aceitarem denúncias por e-mail no endereço reportphishing@apwg.org.

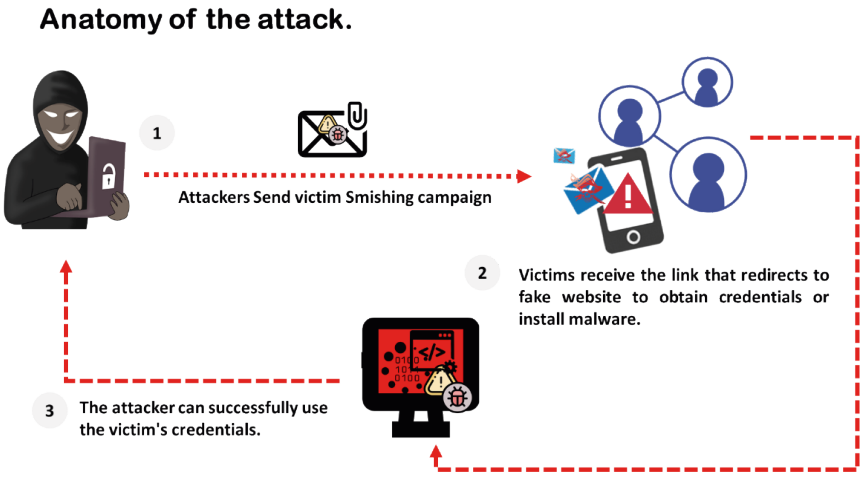
Figura 3
De fevereiro a dezembro de 2019, os totais mensais de incidentes de phishing no Brasil aumentaram impressionantes 232%



Smishing

O smishing é uma técnica de cibercrime derivada do phishing. O termo combina "SMS" com "phishing" e refere-se ao envio de mensagens de texto fraudulentas via SMS ou aplicativos de mensagens multiplataforma. Essas mensagens contêm links com notícias e informações falsas, com o objetivo de capturar senhas e informações pessoais dos destinatários. A imagem a seguir ilustra a anatomia de um ataque de smishing.

Figura 4
Modus operandi de ataque



As campanhas de smishing estão se tornando cada vez mais comuns e sofisticadas. Muitas vezes, elas se disfarçam como mensagens legítimas de instituições financeiras, promoções, prêmios, empresas de serviços ou até mesmo de contatos conhecidos..

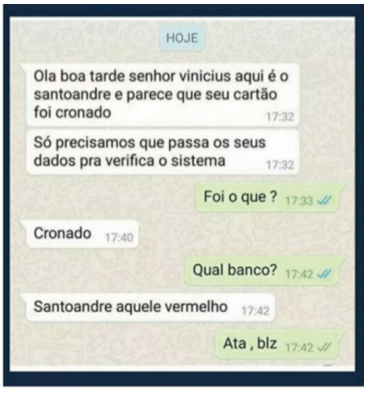
Figura 5
Serviço online de streaming

Para se proteger do smishing, desconfie de mensagens não solicitadas e evite clicar em links ou fornecer informações pessoais. Sempre verifique a autenticidade da mensagem entrando em contato diretamente com a empresa. Nunca compartilhe informações sensíveis por SMS e use software de segurança no seu dispositivo móvel.

Vishing

O vishing, também conhecido como voice phishing, utiliza chamadas telefônicas para enganar as vítimas, em vez de e-mails ou mensagens de texto. Os golpistas se fazem passar por representantes de instituições, agências governamentais ou outras entidades confiáveis, convencendo as pessoas a fornecerem informações pessoais ou financeiras sensíveis.

Figura 6
Exemplo de tentativa de golpe



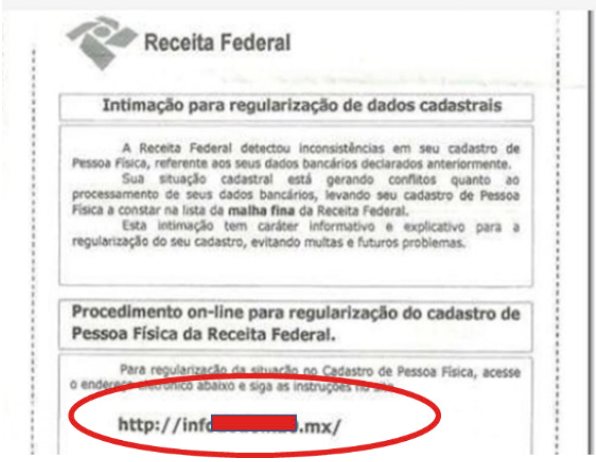
Para se proteger dessa técnica, é importante desconfiar de chamadas não solicitadas e nunca fornecer informações pessoais ou financeiras por telefone. Sempre verifique a identidade do chamador entrando em contato diretamente com a instituição. Evite realizar transferências de dinheiro sem confirmar a solicitação. Utilize tecnologias que bloqueiem chamadas suspeitas, esteja atento a sinais de urgência, monitore suas contas para atividades suspeitas e considere usar serviços de proteção contra fraudes. Em caso de tentativas de golpe, informe as autoridades competentes.

PHISHING "OFFLINE"

Apesar de menos divulgado, o phishing offline é uma tentativa de obter informações pessoais sem o uso de tecnologias digitais. Isso pode envolver o

envio de cartas ou documentos físicos falsos, como faturas, notificações de cobrança ou correspondências bancárias, solicitando que a vítima forneça informações pessoais ou realize pagamentos. Um exemplo comum é o envio de faturas falsas que parecem ser de empresas legítimas, solicitando o pagamento de contas que, na realidade, são fraudulentas.

Figura 7
Exemplo de tentativa de golpe



Sempre verifique a autenticidade de qualquer correspondência que receber. Para fazer isso, entre em contato diretamente com a empresa ou instituição, utilizando as informações de contato oficiais fornecidas por eles.

Dumpster Diving

O "dumpster diving" é uma técnica em que os atacantes vasculham lixeiras ou materiais recicláveis em busca de informações pessoais ou corporativas. Embora não seja uma forma de phishing digital, esses dados podem ser usados para facilitar ataques de phishing mais tradicionais, fornecendo informações que ajudam na personalização dos golpes.

Por exemplo, em um filme, os atacantes são mostrados mergulhando no lixo de uma instituição para obter informações. Depois, eles enviam um e-mail de phishing para um funcionário, que acaba abrindo a mensagem e executando a ação maliciosa, permitindo que os criminosos tenham acesso ao sistema da empresa.

Para evitar que os criminosos obtenham informações sensíveis do lixo, é importante usar trituradores de alta qualidade para destruir documentos e mídias digitais, treinar os funcionários sobre a destruição adequada, estabelecer políticas de retenção e descarte, utilizar serviços profissionais de destruição e instalar caixas de coleta seguras no escritório. Essas práticas ajudam a minimizar o risco de vazamento de informações.

Figura 8
Trecho de obra: Invasores - Nenhum Sistema Está a Salvo

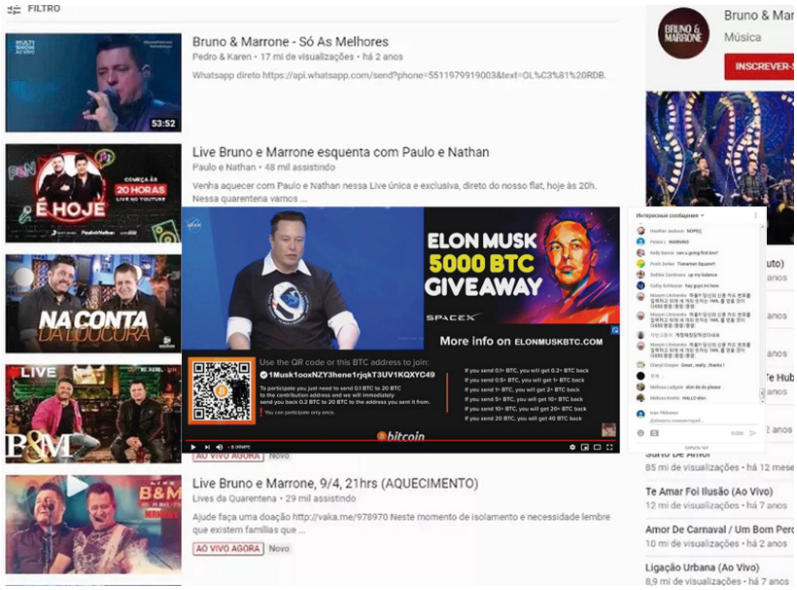
Typosquatting

No typosquatting, os criminosos registram domínios que contenham erros de digitação comuns de websites populares. Quando um usuário digita incorretamente um URL, ele é redirecionado para um site fraudulento. Esses sites podem ser utilizados para instalar malware ou para roubar informações pessoais e financeiras.

Phishing de QR Code

Os golpistas incluem URLs maliciosos em códigos QR. Quando a vítima escaneia o código, seja fisicamente ou virtualmente, ela é redirecionada para um site fraudulento. Esse site pode ser usado para phishing ou para infectar o dispositivo com malware, colocando em risco a segurança do usuário.

Figura 9 – Exemplo



Pharming

Pharming é uma técnica que redireciona os usuários de um site legítimo para uma página fraudulenta sem que eles percebam. Isso geralmente é feito através do envenenamento de DNS ou da manipulação de arquivos de hosts no computador da vítima. Essa prática engana os usuários e captura suas informações pessoais sem o seu conhecimento.

FERRAMENTAS PARA PHISHING

O uso de ferramentas para atacar alvos sem consentimento prévio é ilegal e cabe aos usuários e profissionais de tecnologia obedecer a todas as leis locais. Essas ferramentas são destinadas apenas para fins educacionais e de alerta. Não nos responsabilizamos por qualquer uso indevido, prejuízo ou dano causado.

ShellPhish

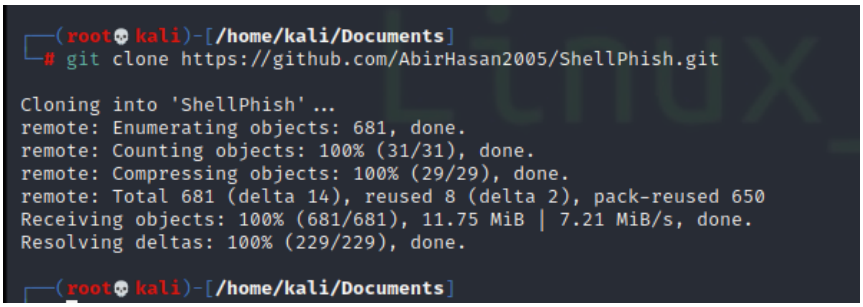
Esta é uma ferramenta de código aberto amplamente utilizada, tornando-se popular para encaminhamento de phishing. Seu objetivo é obter credenciais, como ID e senha. Possui várias versões e oferece modelos de páginas de phishing para mais de 29 mídias sociais, incluindo Instagram, Facebook,

Snapchat, GitHub, Twitter, Yahoo, ProtonMail, Spotify, Netflix, LinkedIn, entre outras.

A ferramenta não está incluída por padrão em distribuições de pentest, como o Kali Linux ou o ParrotOS, e precisa ser baixada do site oficial do GitHub.

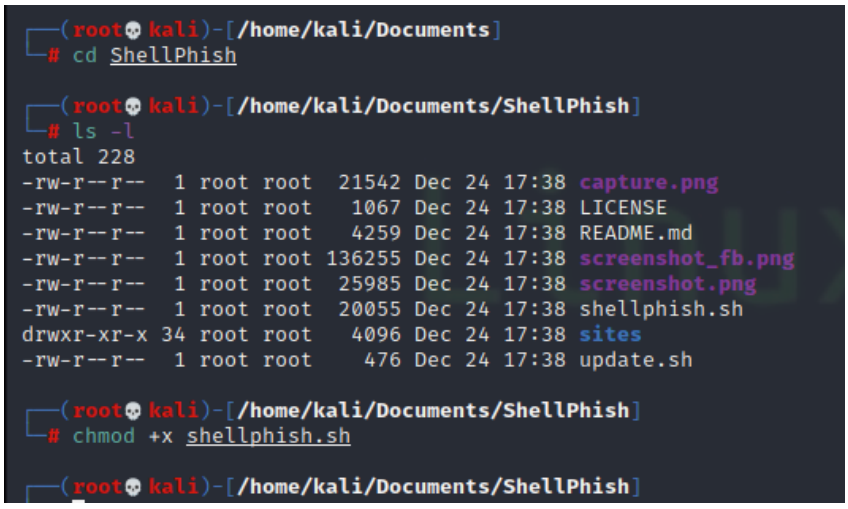
Abra seu Terminal do seu sistema GNU-Linux, escolha um diretório para realizar o download, neste artigo, optou pelo dicuments.

git clone https://github.com/AbirHasan2005/ShellPhish.git



Próximo passo, acesso o diretório com o comado **cd** no diretório Shell-Phish. Após acessar, liste o conteúdo do diretório com o comando **ls -l**.

cd ShellPhish
ls -l



Realizar a mudança na permissão no arquivo Shellphish.sh com o seguinte comando **chmod +x**

```
┌──(root💀kali)-[/home/kali/Documents]
└─# cd ShellPhish

┌──(root💀kali)-[/home/kali/Documents/ShellPhish]
└─# ls -l
total 228
-rw-r--r--   1 root root  21542 Dec 24 17:38 capture.png
-rw-r--r--   1 root root   1067 Dec 24 17:38 LICENSE
-rw-r--r--   1 root root   4259 Dec 24 17:38 README.md
-rw-r--r--   1 root root 136255 Dec 24 17:38 screenshot_fb.png
-rw-r--r--   1 root root  25985 Dec 24 17:38 screenshot.png
-rw-r--r--   1 root root  20055 Dec 24 17:38 shellphish.sh
drwxr-xr-x 34 root root   4096 Dec 24 17:38 sites
-rw-r--r--   1 root root    476 Dec 24 17:38 update.sh

┌──(root💀kali)-[/home/kali/Documents/ShellPhish]
└─# chmod +x shellphish.sh

┌──(root💀kali)-[/home/kali/Documents/ShellPhish]
```

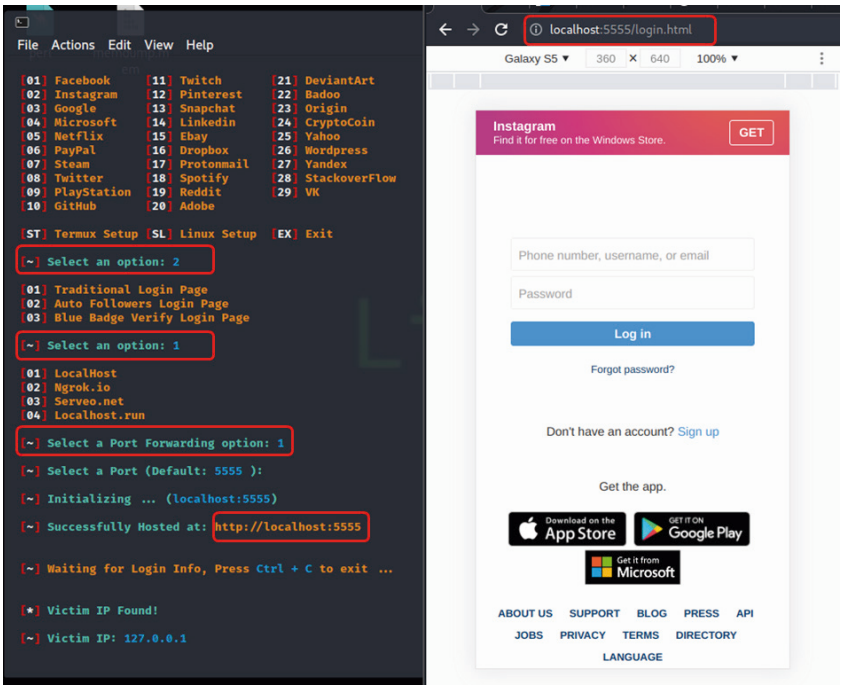
Agora que as configurações estão prontas para uso, vamos executar a ferramenta shellphish executando o seguinte comando em seu terminal bash shellphish.sh ou ./shellphish.sh. Além disso, execute o comando com root.

```
                v2.5-MOD

      .:.:. Phishing Tool Moded by @AbirHasan2005 .:.:.

:: Disclaimer: Developers assume no liability and are not   ::
:: responsible for any misuse or damage caused by ShellPhish ::

.:. Choose any social site which you want to hack .:.

[01] Facebook      [11] Twitch       [21] DeviantArt
[02] Instagram     [12] Pinterest    [22] Badoo
[03] Google        [13] Snapchat     [23] Origin
[04] Microsoft     [14] Linkedin     [24] CryptoCoin
[05] Netflix       [15] Ebay         [25] Yahoo
[06] PayPal        [16] Dropbox      [26] Wordpress
[07] Steam         [17] Protonmail   [27] Yandex
[08] Twitter       [18] Spotify      [28] StackoverFlow
[09] PlayStation   [19] Reddit       [29] VK
[10] GitHub        [20] Adobe

[ST] Termux Setup [SL] Linux Setup  [EX] Exit

[~] Select an option: 2

[01] Traditional Login Page
[02] Auto Followers Login Page
[03] Blue Badge Verify Login Page

[~] Select an option: 1

[01] LocalHost
[02] Ngrok.io
[03] Serveo.net
[04] Localhost.run

[~] Select a Port Forwarding option: 1
```

Step1 - precisamos escolher a opção que será utiliza para envio. Optamos pela opção de número 2 que é o Instagram.
Step 2- Em seguinte, optamos pela opção de número 1, “Tradicional login page”.
Step 3 -A ferramenta solicita a opção de servidores que será utilizado para o encaminho do link. Neste nosso exemplo, afim demonstrativo, optamos pela opção 1, “LocalHost.”

Step 4 - Precisamos escolher a porta, por padrão é 5555, vamos usar a configuração padrão e digitar enter.

O Shellphish automatiza o processo de inicialização dos serviços, fornecendo a URL a ser utilizada. Neste caso, foi usado em um laboratório para conduzir uma campanha interna de conscientização em uma instituição. Para demonstrar o funcionamento da ferramenta, o link foi aberto no navegador do próprio servidor.



SmishingTools

Outra ferramenta com objetivo de realizar disparo de SMS, desenvolvida em HTML e Python por Ishan Saha, no qual, não está nos repositórios oficiais do GNU-Linux, tento que realizar o download do repositório oficial na página do github (https://github.com/ishan-saha/SmishingTool). Requer a utilização da API gratuita do fast2sms (https://www.fast2sms.com), para realizar o envio do SMS, no qual, realiza o tunelamento com ngrok, em conjunto com seu Micro Framework Web flask.

CONCLUSÃO

A conscientização sobre as diversas formas de phishing e suas variantes é essencial para mitigar os riscos associados a estas ameaças. Compreender as táticas usadas pelos cibercriminosos, como Spear Phishing, Vishing, Phishing Offline, Dumpster Diving, Typosquatting, Phishing de QR Code, Pharming e Encurtadores de Link, permite que tanto indivíduos quanto organizações se preparem melhor para se defender contra essas fraudes.

A adoção de práticas de segurança robustas, como a educação contínua dos colaboradores, a implementação de sistemas de autenticação multifator, a realização de auditorias regulares e a atualização constante de softwares de segurança, pode reduzir significativamente as vulnerabilidades. Além disso, fomentar uma cultura de segurança cibernética dentro das empresas e no uso pessoal é crucial para enfrentar os desafios deste cenário em constante evolução.

Portanto, à medida que a tecnologia avança, é imperativo que todos se mantenham informados e vigilantes, adotando medidas proativas para proteger seus dados e sistemas. A segurança da informação não é apenas uma responsabilidade dos especialistas, mas um compromisso compartilhado por todos os usuários de tecnologia. Somente assim, poderemos estar um passo à frente dos cibercriminosos, garantindo um ambiente digital mais seguro e resiliente para todos.

Capítulo 6
Como a Prova Digital e a Negociação Coletiva do Trabalho se Relacionam

Luiz Eduardo Gunther
Marco Antônio César Villatore

1. INTRODUÇÃO

As novas tecnologias de comunicação e informação causaram grande impacto no Direito do Trabalho. Especialmente pela rapidez com que aconteceram. São as imagens, a voz, os textos, tudo é transmitido em tempo muito rápido.

A indagação que se pretende responder é como a prova constituída no meio digital pode ser relevante para a negociação coletiva do trabalho. Essa prova normalmente produzida extrajudicialmente, no mundo da vida, e que depois pode ser examinada no ambiente judicial.

Como se sabe, a prova é um instrumento fundamental na aplicação do Direito e da Justiça. E a prova digital, naturalmente, apresenta aspectos essenciais, que a diferenciam da prova tradicional, a prova histórica, que se construiu em tempo analógico.

Quais os aspectos relativos à prova que devem se apresentar para uma compreensão melhor do que acontece no mundo digital? Quais os aspectos de uma teoria geral da prova que permanecem. Conceito? Características? Fundamentos? Exigências para a validação? O que é necessário estabelecer como premissas para garantir que a prova digital possa ser aceita, aplicada e reconhecida no meio judicial?

Para reconhecer esses aspectos há que se passar por doutrinadores que se debruçaram com rigor metodológico sobre o tema, analisando, inclusive, a temática filosófica prova versus verdade.

Para fazer uma ligação mais profunda com o Direito e a Justiça do Trabalho optou-se pelo estudo da negociação coletiva e a prova digital. O que se compreende por negociação coletiva do trabalho? Qual a sua importância

e impacto nas relações de trabalho? Ela foi afetada pelo mundo digital, pela existência de uma prova com aspectos tecnológicos? Quais os aspectos que hoje já se descortinam para uma negociação coletiva realizar-se com aplicação de tecnologias digitais?

2. ASPECTOS IMPORTANTES RELACIONADOS À PROMOÇÃO DA PROVA DIGITAL

Quando se estuda o fenômeno da prova como instituto, deve-se indagar qual o seu significado, a sua definição. Cumpre, então, reconhecer seu caráter multifacetário, capaz de imprimir à figura, conforme o prisma através do qual se a observa, diferentes nuances. Desse modo, tem-se que a prova pode resumir-se em um aspecto argumentativo-retórico, apto a justificar a escolha de uma das teses apresentadas pelas partes no processo.

Em outras palavras, a prova assume a função de fundamento para a escolha racional da hipótese destinada a constituir o conteúdo da decisão final sobre o fato. Assim, é possível definir a prova, em direito processual, como "todo meio retórico, regulado pela lei, e dirigido, através dos parâmetros fixados pelo direito e de critérios racionais, a convencer o Estado-juiz da validade das proposições, objeto de impugnação, feitas no processo". (MARINONI, 2009, p. 57)

Ressalte-se, sempre, a fundamentalidade do direito à prova. O direito à prova constitui manifestação do direito de acesso à justiça, à defesa, ao contraditório, à justa solução dos conflitos submetidos ao Poder Judiciário e à efetividade da jurisdição e do processo, sendo todos esses direitos também reconhecidos pelo Direito Internacional dos Direitos Humanos.

Pondere-se, igualmente, que, ao reconhecer o direito à dignidade humana e, com isso, aos diretos a ela inerentes, o Direito Internacional dos Direitos Humanos reconhece o direito à prova, vez que "não há titularidade real de direitos sem a possibilidade concreta de fazê-los valer, quando não respeitados espontaneamente. Não há dúvida, assim, que, "negar o acesso aos direitos é negar a sua titularidade e, com isso, o próprio valor da pessoa humana". O direito à prova, portanto, é "uma exigência da dignidade humana, reconhecida pelo Direito Internacional dos Direitos Humanos a toda e qualquer pessoa humana". (ALMEIDA, 2013, p. 186)

Sobre o tema verdade e processo, muito se escreveu, e ainda muito se escreverá. Naturalmente que quando se menciona a "prova digital" essa análise deve continuar sendo relevante. Ao apreciar a prova, o julgador não se limita a constatar que ela revelou a existência ou inexistência de um fato, a verdade ou a falsidade de uma afirmação. Pergunta sobre a inferência que a prova, por si mesma, terá na sentença.

Assume, desse modo, uma postura crítica, examinando os atributos da prova, procurando desvendar o que há de intrínseco nela. Devemos compreender, porém, que, "na valoração, pode ocorrer a necessidade de avaliar-se a prova, ou seja, confrontá-la com outra é julgá-la em função dessa comparação". Entretanto, "a prevalência é sempre da operação de valorar, que encerra a essência do ato de julgamento." (PAULA, 2010, p. 62)

Para que a prova digital seja útil e válida, é necessário que reúna os seguintes requisitos: a) autenticidade; b) integridade; c) presunção da cadeia digital. Ausentes quaisquer dos requisitos ou pressupostos, a prova mostrar-se-á frágil, ou até mesmo imprestável para produzir efeito no processo.

Por **autenticidade** deve-se entender a qualidade da prova digital que permite a certeza com relação ao autor ou autores do fato digital. Já **integridade** pode ser entendida como a qualidade da prova digital que permite a certeza com relação à sua completude ou não adulteração. Preservar a **cadeia de custódia** da prova digital, desde sua identificação até sua apresentação no procedimento de destino. (GOMES, 2023, p. 63-62)

Inúmeras questões surgem com o eventual uso da prova, ou da perícia, de geolocalização. Há invasão de privacidade? Pode ocorrer violência ao direito à intimidade?

Do mesmo modo, quando se pretende fazer prova dos algoritmos utilizados nas plataformas digitais poderia haver violação ao segredo industrial, criando a possibilidade de concorrência desleal.

Naturalmente, toda essa temática ainda está em início, muitas ponderações e decisão ocorrerão, nos próximos anos, sobre esses aspectos, que também envolverão as câmeras digitais, a discriminação nos controles por reconhecimento facial, e assim por diante.

3. COMO SE PODE UTILIZAR NA NEGOCIAÇÃO COLETIVA DO TRABALHO INSTRUMENTOS EFICAZES RELACIONADOS À PROVA DIGITAL

As relações capital-trabalho foram reestruturadas no início da era da informação, com as imensas transformações ocorridas.

Esse fenômeno resultou de circunstâncias históricas, oportunidades tecnológicas e imperativos econômicos. Com o objetivo de reverter a diminuição dos lucros sem causar inflação, as economias nacionais e empresas privadas passaram a atuar sobre os custos da mão-de-obra desde o início dos anos 80, de duas formas principais: a) mediante o aumento da produtividade sem criação de empregos (principais economias da Europa); b) desvalorização de um grande número de novos empregos (Estados Unidos). Dentro dessas circunstâncias, os sindicatos de trabalhadores, que se constituíam em principal

obstáculo à estratégia unilateral de reestruturação foram enfraquecidos por sua incapacidade de representar os novos tipos de trabalhadores (mulheres, jovens, imigrantes), de atuar em novos locais de trabalho (escritórios do setor privado, indústrias de alta tecnologia) e de funcionar nas novas formas de organização – a empresa em rede em escala global. (CASTELLS, 1999, p. 349-350)

Essas mudanças causaram grande impacto na existência dos entes sindicais coletivos de trabalhadores, que tiveram grande dificuldade em adaptar-se.

Qual será o papel a ser assumido pelo Estado, pelas empresas e pelos entes coletivos nessa mutação do trabalho que está ocorrendo na segunda década do século XXI?

É possível relacionar algumas importantes funções da negociação coletiva: compositiva; criação de normas, obrigações e direitos. Provavelmente, a maior funcionalidade da negociação, aquela pela qual sempre se reconhece como fundamental, é a **compositiva**, pela qual os conflitos entre as partes são superados, harmonizando os interesses contrapostos dos trabalhadores e dos empregadores. A **criação de normas**, igualmente, se insere como uma das funcionalidades da negociação, que se aplicarão às relações individuais de trabalho. **Criar obrigações e direitos entre os próprios sujeitos estipulantes**, sem reflexo sobre as relações individuais de trabalho, estabelecendo deveres e faculdades a serem cumpridas pelos entes coletivos.

Todas essas funções receberam grande impacto do mundo digital. O avanço tecnológico e a informática criaram um mundo dos computadores, disponibilizaram mão de obra, "novas profissões surgiram, privatizações de empresa públicas intensificaram-se, sempre com profundas alterações nas relações de trabalho e no poder dos sindicatos perante o empregador". (NASCIMENTO, 2009, p. 484-490).

Os trabalhadores, e os seus sindicatos, não são convidados de pedra na negociação coletiva. São eles os destinatários principais desse fenômeno típico do capitalismo.

Não parece haver qualquer dúvida que o direito e o dever da informação, ou da transparência, como princípio jurídico, é essencial à negociação coletiva, na qual, os trabalhadores, por intermédio de seus sindicatos, e os empresários (com ou sem seus sindicatos patronais) "apresentam-se na arena dos conflitos coletivos, enxergando-se uns aos outros não como oponentes, mas como partes interessadas em encontrar um ponto comum para solucionar as divergências existentes". (GUNTHER; VILLATORE, 2022, p. 962)

Às vezes pode-se imaginar a perda de importância da atividade sindical com a globalização e o incremento do mundo digital. Isso, na verdade, não acontece, pois longe de haver perdido centralidade, "as formas organizacionais vinculadas à representação sindical vêm sendo reconfiguradas incessantemente", emulando práticas corporativas em rede, mas também se desenvolvendo a

partir de repertórios históricos e inovações institucionais. Nesse contexto, em grande medida, o debate internacional sobre o escalonamento da ação coletiva sindical vem demonstrando "o renovado potencial político dos sindicatos e sua contínua capacidade de pautar a agenda pública em torno da melhoria das condições e relações de trabalho. (RAMALHO; SANTOS, 2022, p. 850)

A negociação coletiva não está imune à influência, a nível de conteúdo e procedimento, do processo de digitalização dos contextos produtivos. "Nos setores já sujeitos à negociação na era pré-digital, a mutação provocada pelo advento da informatização avançada e das novas tecnologias produziu, principalmente, uma modificação dos conteúdos entre parceiros sociais;" (AVOGARO, 2020, p. 32-47)

Qual é o papel efetivo do sindicato quando se trata da proteção de dados dos trabalhadores, seja na criação de normas coletivas, seja atuando judicialmente?

No explicar de Luciane Cardoso Barzotto, tanto na negociação autônoma, quando no Sindicato produz fonte de Direito do Trabalho, como na ação judicial para assegurar direitos de proteção de dados, há uma autorização legal para a atuação sindical em questão de proteção de dados, especialmente no interesse da categoria, em situações de evidentes violações a direitos individuais homogêneos, como seria o resguardo de dados de uma determinada coletividade laboral de eventual incidente de segurança ou violação do tratamento legal em desconformidade com a finalidade declarada pelo controlador.

Por esses motivos, será possível, viável e legal a existência de "cláusula convencional prevendo a autorização de envio de dados dos trabalhadores aos sindicatos pela categoria econômica, cuja autorização foi feita em assembleia geral e em conformidade com a vontade dos associados." (BARZOTTO, 2021, p. 159)

Quando se aprofunda o tema da negociação coletiva não há como deixar de concluir que se trata de um dos momentos mais importantes da atividade sindical, onde se apresentam a cidadania e a democracia. Ambas as palavras expressam participação na melhor condição do trabalho e das trabalhadoras e dos trabalhadores.

Por outro lado, com a vinda do mundo digital, especialmente o teletrabalho, tanto a cidadania como a democracia passaram a ser ainda mais relevantes pela exigência da participação efetiva de quem trabalha na discussão e implementação de normas coletivas, que podem realmente aprimorar as relações de trabalho. A democracia digital promove a democracia interna das entidades sindicais, com a verticalização do debate e facilitação da participação dos interessados.

Desse modo, a formação de opinião e expressão consolidada da somatória das opiniões particulares, daqui para frente, "consistirá na construção da vontade coletiva, irremediavelmente, mediada pelo uso dos aparatos tecnológicos para reunião, consulta e deliberação por plataformas ou ferramentas *online*". (NICOLADELI; ALMEIDA; CARLESSO, 2022, p. 923)

Considera-se que o emprego das facilidades oferecidas pelas tecnologias aos sindicatos deve ter as seguintes premissas: a) nenhuma tecnologia substitui plenamente o contato sindical presencial com a base; b) as tecnologias devem facilitar o acesso da base às entidades, promovendo e facilitando o diálogo; c) a tecnologia deve servir à representação sindical, não podendo ser utilizada para finalidade diversa; d) a tecnologia deve abranger todos os representados, não apenas uma cúpula política ou de abastados em recursos tecnológicos; e) as homologações nas rescisões e os cálculos indenizatórios devem ter tratamento especial, rápido e transparente aos trabalhadores. Os instrumentos tecnológicos, assim, devem se pautar na finalidade da função sindical, nos interesses da categoria e na atividade de representação. Não seria apropriado, desse modo, que "as tecnologias se voltassem apenas para dentro da entidade, como forma de cobrar contribuições ou somente facilitar o trabalho administrativo interno". (LIMA, 2022, p. 725-726)

Será possível realizar negociação coletiva à distância, com utilização do aparato digital? Devem, sem dúvida, os sindicatos mapear as respectivas categorias e profissões, fazendo juízo de futurologia no sentido de verificar quais ameaças pairam no ar e quais proteções são adequadas aos trabalhadores.

Algumas cláusulas se mostram essenciais, nestes tempos "como a implementação do direito à desconexão e a que assegure direito de defesa na exclusão dos trabalhadores de plataforma". Direitos mínimos aos que trabalham sem vínculo de emprego ou sob condições de pressão e opressão devem ser assegurados "nas negociações coletivas, já que a tendência do Estado é se afastar das relações laborais. É preciso pensar em cláusulas que reduzam o impacto ou os efeitos da tecnologia". (LIMA, 2022, p. 728)

O advento das relações de trabalho mediadas pelos algoritmos trouxe à baila novas modalidades de discriminação indireta (por filtros, por aprendizagem ativa, por tratamento aleatório-randômico), que devem ser debeladas por todas as vias institucionais disponíveis, especialmente a via da negociação coletiva. (FELICIANO, 2023, p. 257-270)

Constituem desafios e aspectos relevantes do teletrabalho novas pautas de negociação coletiva que, segundo a Organização Internacional do Trabalho (OIT), por intermédio das Notas Técnicas 6/6/2021 e 6/7/2021, seriam as seguintes, em síntese, dentre outras: a) o uso da tecnologia e da Inteligência Artificial a favor do sindicalismo, na defesa da categoria, e para operacionalizar o direito à informação, consulta e negociação coletiva e diálogo coletivo; b) pautas sobre os imperativos das novas tecnologias, de novas competências humanas, de qualificação e requalificação profissional; c) "negociação coletiva para proteção dos direitos de personalidade e combate à violência e assédio moral e digital denominados *gaslighting*, *manterrupting*, *mainsplaing*, *bropriating* e as novas modalidades de *bullying* digital e por algoritmo denominado de *cyberbullying* e *cyberstalking*". (BRAMANTE; BRAMANTE, 2023, p. 522-524)

Deve ser registrado, com ênfase, ainda, que a regulamentação estatal do teletrabalho, em regra, é insuficiente e potencializa o debate na senda da necessidade de complemento normativo via negociação coletiva, especialmente "o direito do teletrabalhador de organização sindical e os impedimentos práticos do exercício dos direitos de representação coletiva e de greve, e também o direito de participação na empresa e outras formas participativas". (BRAMANTE; BRAMANTE, 2023, p. 524-525)

O tema da desconexão ganhou imenso relevo a partir da pandemia da Covid-19, quando o uso do teletrabalho intensificou-se. Passou-se a indagar, então, o que faltava para reconhecer esse direito. Verificou-se que não estavam claramente definidos os parâmetros do que se devia entender por "direito à desconexão".

Essa lacuna legal, no que tange à prerrogativa do trabalhador de permanecer desconectado, poderia, então, ser suprida pelo diálogo social, pois esta é, justamente, uma das funções primeiras da negociação coletiva, ou seja, a regulação setorial, pautada nas necessidades específicas de determinado segmento ou empresa.

Entretanto, pesquisa realizada no sistema Mediador do Ministério do Trabalho brasileiro, no mês de agosto de 2023, constatou "a existência de apenas nove instrumentos normativos vigentes com cláusulas específicas destinadas ao direito de desconexão". Como se há de compreender, trata-se de número irrisório, se considerarmos que, no ano, registraram-se em torno de 7.400 (sete mil e quatrocentos) instrumentos coletivos nesse sistema. (FREIRE, 2023, p. 24)

O novo mundo do trabalho, que já está a nossa volta, precisa receber consideração especial dos entes coletivos. Nesse sentido, a ideia do viés coletivo sindical do século XXI não é apenas para servir de representante (como nos tempos analógicos) de um certo número limitado de trabalhadores (empregados) de um determinado setor, mas trabalhar na construção de um bloco de interesses, afetos, diálogos, experiências, aos quais o maior número de trabalhadores adira, "numa espécie de condensador, agregador de sujeitos e ideias, em constantes aproximações, diversidade, adesões e desgarramentos, transformando-se para tanto em contato ativo com outros centros de intensidade". (AGUIAR, 2023, p. 371)

Passa-se, assim, do analógico ao digital. De uma demonstração de fatos com registros em papel para um novo descortinar da vida digital e sua capacidade mais adequada de demonstrar os fatos da vida.

A Lei Geral de Proteção de Dados é um marco civilizatório no Brasil e ainda apresenta os seus primeiros passos. Questiona-se se é possível os sindicatos judicializarem aspectos relacionados à LGPD, em seus ângulos jurídicos e econômicos. Desse modo, trata-se de lançar luz sobre a representação eficaz dos interesses dos empregados, quanto à legitimidade ativa dos sindicatos nas ações trabalhistas envolvendo a LGPD.

Deve-se, sem dúvida, buscar equilibrar a necessidade de justiça individual com os interesses coletivos, pois aí se desenvolve uma teia complexa de considerações legais e éticas. Nesse sentido, "os Tribunais enfrentam o desafio de discernir entre a busca genuína pela proteção à privacidade da coletividade e a possível exploração de oportunidades para ganho institucional". (ARAÚJO, 2023, p. 410)

Um trabalho de pesquisa muito interessante analisou o sindicalismo e a negociação coletiva trabalhista nas plataformas digitais de consumo, levando em conta a situação fática e jurídica dos divulgadores digitais. Nesse estudo, asseverou-se que, embora existam desafios a serem ultrapassados, para se garantir acesso sindical aos trabalhadores que atuam como divulgadores de empresas do ramo do comércio varejista de bens, considerou-se necessário que as entidades sindicais da categoria busquem meios para alcançá-los, de modo que as suas demandas passem a compor, obrigatoriamente, "as pautas de reinvindicação da categoria dos comércios, com intuito de reafirmar o sistema constitucional e legal de proteção trabalhista edificado na premissa básica do direito fundamental ao trabalho digno". (DELGADO; DIAS; ASSIS, 2022, p. 1.005)

Segundo Sidnei Machado, não há registro de experiências no Brasil de atuações visando ao estabelecimento de processo de negociação coletiva, ou mesmo a reinvindicação de estabelecimento de um código de conduta pelas plataformas digitais, "com padrões de trabalho justo, que reforcem as melhores práticas na relação entre plataformas digitais e seus prestadores de serviços". (MACHADO, 2022, p. 754).

Não parece haver controvérsia no sentido que o mundo digital dirige-se à melhoria de qualidade de vida dos trabalhadores, com mais saúde, menos riscos, com respeito àquilo que se denomina trabalho decente, expressão cunhada pela Organização Internacional do Trabalho – OIT. Assim, as alterações havidas no universo do trabalho por conta da evolução tecnológica devem servir pra fomentar o desenvolvimento de novos mecanismos de proteção de direitos da pessoa que trabalha, mantendo-se em mente as funções e o alcance do direito do trabalho, do direito coletivo e da atuação sindical.

4. CONSIDERAÇÕES FINAIS

Buscou-se no texto entender o mecanismo da prova digital sob a perspectiva jurídica, sua compreensão, conceito, características, fundamentos, aspectos necessários para reconhecer sua validação.

Ao mesmo tempo, delinearam-se aspectos essenciais da negociação coletiva do trabalho no mundo digital.

O surgimento de atividades como o teletrabalho, labor em plataformas digitais, como exemplos, mostram o surgimento de novas perspectivas no mundo do trabalho.

Como levar o exercício das atividades sindicais para o universo da tecnologia? Como trazer aspectos essenciais à compreensão da prova digital para a vida sindical, especialmente o exercício da negociação coletiva?

Essas indagações são recentes porque o significado para prova digital ainda é novo, e porque a negociação coletiva do trabalho, que possui construção de décadas, ainda não incorporou as novas tecnologias, que poderiam facilitar e aprimorar o diálogo social.

REFERÊNCIAS

AGUIAR, Antonio Carlos. Novos arquétipos sindicais. *In* AZEVEDO NETO, Platon Teixeira de; BITTENCOURT, Renata Osório Caciquinho; OLIVEIRA, Gustavo Afonso (Coord.). **Direito Coletivo do Trabalho**. Brasília-DF: Editora Venturoli, 2023. p.363-374.

ALMEIDA, Cleber Lúcio de. **Elementos da Teoria Geral da Prova:** a prova como direito humano e fundamental das partes do processo judicial. São Paulo: LTr, 2013.

ALMEIDA, Isis de. **Teoria e prática das provas no processo trabalhista**. São Paulo: LTr: Ed. da Universidade de São Paulo 1980.

ARAÚJO, Bruna de SÁ. A judicialização da LGPD pelos sindicatos: aspectos jurídicos e econômicos. *In* AZEVEDO NETO; Platon Teixeira de; BITTENCOURT, Renata Osório Caciquinho; OLIVEIRA, Gustavo Afonso (Coord.) **Direito Coletivo do Trabalho**. Brasília-DF. Editora Venturoli, 2023.

AVOGARO, Matteo. Direitos coletivos, tratamento do direito sindical e convênios. *In* LUDOVICO, Giuseppe; FITA ORTEGA, Fernando; NAHAS; Thereza Christina (Coord.). **Novas tecnologias, plataformas digitais e direito do trabalho**: uma comparação entre Itália, Espanha e Brasil: São Paulo: Thomson Reuters Brasil, 2020. p. 13-48.

BARZOTTO, Luciane Cardoso. LGPD e desafios recentes da negociação coletiva no Brasil. *In* SILVA NETO, Manoel Jorge (Org.). **Desafios à autonomia negocial coletiva**: estudos em homenagem ao Professor José Augusto Rodrigues Pinto. Brasília-DF: ESMPU, 2021, p.148-172.

BRAMANTE, Ivani Contini; BRAMANTE, Simone. Teletrabalho e Negociação Coletiva. *In* FELICIANO, Guilherme Guimarães; LIMA, Patrícia Helena Azevedo; MATOS, Larissa (Org.). **Os desafios do teletrabalho**. Campinas-SP: Lacier Editora, 2023. p.511-527.

CASTELLS, Manuel. **A sociedade em rede** – Vol I. 14. reimpressão. Trad. Roneide Venancio Majer com a colab. De Klaus Brandini Gerhardt. São Paulo? Paz e Terra, 1999.

DELGADO, Gabriela Neves; DIAS, Valéria de Oliveira; ASSIS, Carolina de. Sindicalismo e negociação coletiva trabalhista nas plataformas digitais de consumo: uma análise da situação fática e jurídica dos divulgadores digitais. In DELGADO, Maurício Godinho *et al*. **Democracia, sindicalismo e justiça social**: parâmetros estruturais e desafios no século XXI. São Paulo: Editora Juspodium, 2022, p. 985-1007.

FELICIANO, Guilherme Guimarães. **Proteção de dados pessoais e os impactos nas relações de trabalho**: princípios, aplicações e crítica. São Paulo: Thomson Reuters Brasil, 2023.

FREIRE, Gisele da Silva. O direito à desconexão no trabalho na era digital: necessidade de regulamentação no Brasil. **Revista do Advogado.** n. 160, dez. 2023, AASP, p. 19-26.

GOMES, Erika Cristina Ferreira. Provas digitais e sua repercussão no Direito Processual do Trabalho. **Revista Trabalhista Direito e Processo**, Ano 20, n. 65, janeiro-junho 2021. São Paulo, LTr, julho 2023. p. 56-68.

GUNTHER Luiz Eduardo; VILLATORE, Marco Antônio César. O princípio do direito e dever da informação ou da transparência na negociação coletiva trabalhista. *In* DELGADO, Mauricio Godinho *et al*. **Democracia, sindicalismo e justiça social**: parâmetros estruturais e desafios no século XXI. São Paulo: Editora Juspodium, 2022. p. 947-964.

LIMA, Francisco Gérson Marques de. Tecnologia e o futuro dos sindicatos. *In* DELGADO, Mauricio Godinho *et al* (Org.) p.725-726. **Democracia, sindicalismo e justiça social**: parâmetros estruturais e desafios no século XXI. São Paulo: Editora Juspodium, 2022. p. 719-730.

MACHADO, Sidnei. Representação coletiva dos trabalhadores em plataformas digitais. *In* DELGADO, Mauricio Godinho *et al* (Org.). **Democracia, sindicalismo e justiça social**: parâmetros estruturais e desafios no século XXI. São Paulo: Editora Juspodium, 2022. p. 749-755.

MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz. **Prova**. São Paulo: Editora Revista dos Tribunais, 2009.

NASCIMENTO. Amauri Mascaro. **Compêndio de Direito Sindical**. 6. ed. São Paulo: LTr, 2009.

NICOLADELI, Sandro Lunard; ALMEIDA, João Guilherme Walski de; CARLESSO, Adriano. Negociações coletivas e assembleias sindicais na pandemia: aspectos peculiares da democracia sindical digital. *In* DELGADO, Maurício Godinho *et al.* **Democracia, sindicalismo e justiça social**: parâmetros estruturais e desafios no século XXI. São Paulo: Editora Juspodium, 2022. p.911-924.

PAULA, Carlos Alberto Reis de. **Especificidade do ônus da prova no processo do trabalho**. 2. ed. São Paulo: LTr, 2010.

RAMALHO, José Ricardo; SANTOS, Rodrigo Sales Pereira dos Trabalho e ação sindical em redes globais de produção. *In* DELGADO, Mauricio Godinho *et al*. **Democracia, sindicalismo e justiça social**: parâmetros estruturais e desafios no século XXI. São PAULO: Editora Juspodium, 2022. p.815-833.

Capítulo 7

Doença Mental, Crime e Tecnologia: O Neurofeedback como Técnica de Reeducação da Personalidade Criminosa

Alexandra Rodrigues de Souza Cruz
Guilherme Rodrigues de Souza Cruz

INTRODUÇÃO

O entendimento acerca do comportamento delinquente é muito mais complexo do que os conceitos criados isoladamente pelas diversas Ciências. Para se atingir o cerne do delinquente, é necessária uma análise conjugada de diversos aspectos que permeiam a humanidade, e o auxílio das mais diversas áreas do conhecimento.

A Pesquisa que ensejou a produção deste artigo nasceu de indagações acerca da situação inerte dos criminosos nas casas penais, sejam elas de tratamento médico ou penitenciárias. Questiona-se o que fazer com estes indivíduos uma vez que eles são colocados sob a guarda estatal? Diante da vagueza e incompletude lesgislativa, como saber para onde enviar pessoas que cometem crimes violentos? Ou mesmo, psicopatas e assassinos em série? E, uma vez alocados em casas penais, como tratá-los ou ressocializá-los?! Buscou-se responder a tais questionamentos buscando informações interdisciplinares no Direito, na Psquiatria, na Psicanálise e também na computação aplicada à medicina neural.

Para tanto, realizou-se pequisa de cunho teórico na literatura jurídica e psicológica a cerca de quais seriam os principais fatores para o comportamento criminoso e de como o Estado tem lidado com tais indivíduos através do Direito Penal; analisando, portanto, sua imputabilidade e o tratamento penal atribuído aos mesmos. De posse de tais informações e, em um segundo momento, recorreu-se ao apoio das ciências tecnológicas para, através de pesquisas teóricas, com respaldo de dados empíricos; alcançar e compreender as possibilidades da medicina moderna e automatizada para tratar e reeducar tais indivíduos.

Concluindo-se, destarte, que o aparelho carcerário estatal padece de séria deficiência no que compete à identificação e tratamento de indivíduos com tendência a comportamentos criminosos e, apontando-se, com base na melhor doutrina e em análises empíricas, soluções possíveis e indicadas para tal problemática; como a inovadora técnica de neurofeedback cerebral.

1. FATORES BIOPSICOSSOCIAIS DO COMPORTAMENTO DELINQUENTE

Desde épocas remotas, pesquisadores e estudiosos de diversas Ciências buscam explicar as causas do comportamento criminoso. Criminologia, Sociologia, Antropologia, Psicologia e outras, tentam responder a uma mesma pergunta: " Por que o ser humano pratica crimes"? Ocorre que, o crime é um fenômeno tão complexo que para ser explicado requer profunda interdisciplinaridade. Portanto, no que se refere ao ser humano, pode-se concluir que o comportamento criminoso se dá por fatores biológicos, psicológicos e sociais.

Cesare Lombroso (2013), atualmente, é considerado por muitos como "ultrapassado", uma vez que estabeleceu características biológicas que supostamente poderiam indicar um criminoso. Entretanto, a Ciência considerada moderna já confirmou que, de fato, diversos elementos biológicos podem influenciar no comportamento criminoso, tais como: fatores hormonais, metabólicos, congênitos e hereditários. Em verdade, sabe-se que a hereditariedade chega a influenciar em cerca de 40 a 50% o comportamento de um indivíduo para que venha a se tornar delinquente (Raine, 2008). Em termos hormonais, por exemplo, também já restou comprovado que em razão da presença de hormônios como a testosterona serem mais evidentes em indivíduos do sexo masculino, é muito mais frequente a prática de crimes por homens do que por mulheres. Assim também, é maior o índice de criminalidade perpetrada por jovens do que por pessoas de idade mais avançada; e boa parte da explicação para este fato social é de que os jovens possuem maior concentração hormonal (Daly; Wilson, 1988).

Mas, ainda que não se possa escapar no destino biológico, nem tudo está perdido. Ouso discordar de Lombroso e dizer que não nascemos criminosos! Isto porque, existem ainda outros dois aspectos do comportamento humano que podem influenciar na formação do criminoso: O psicológico e o social.

Do ponto de vista psicológico, sabe-se que o indivíduo pode vir a desenvolver diversos transtornos de personalidade que o aproximem da vida criminosa. Não quer dizer que todo o criminoso possua transtornos de personalidade, mas certamente a presença destes podem desaguar em condutas delitivas. Ainda que não haja o diagnóstico de um transtorno ou qualquer tipo de psicopatologia, traços psicológicos que compõem a personalidade do

agressor também podem conduzi-lo ao caminho do crime, como: pouca capacidade de retardar o prazer, baixa empatia, esquemas cognitivos agressivos, falha na discriminação entre eventos passados e atuais, errôneas estimativas e interferências cognitivas, sentimentos de ira e hostilidade diante de situações de frustração e provocação, autoestima instável, ideias neutralizadoras sobre as consequências de seus atos e etc...(Lino, 2021).

Por fim, há de se atentar, ainda, para os diversos fatores sociais que podem influenciar no desenvolvimento da criminalidade. Para os que acreditam em Deus, destino ou qualquer força maior que determine o ambiente onde o ser humano será gerado e nascido; certamente poderão afirmar que parcela da determinação acerca de futuras condutas delitivas advém de fatores sociais como: a desorganização da comunidade na qual se está inserido, a desigualdade de oportunidades, os estereótipos sexuais, a aceitação da violência e etc. Sem deixar de se mencionar a primeira sociedade na qual o homem se insere, qual seja, a familiar. Indivíduos com laços familiares deficientes, nascidos em famílias de baixa instrução e/ou renda, que tenham modelos paternos violentos e desorganização familiar; certamente possuem maior probabilidade de vir a desenvolver comportamentos criminosos (Picolotto, 2017).

Não é possível afirmar, portanto, que todo criminoso possui algum tipo de alteração mental; assim como não há que se estabelecer que todo doente mental ou pessoa com transtorno de personalidade venha a praticar crimes. Mas certamente, a fronteira entre ambos é delimitada por uma linha bastante tênue. Assim, o estudo do Direito Penal hodierno implica, necessariamente, no estudo psiquê humana.

2. DIREITO PENAL E DOENÇA MENTAL: CRIME E LOUCURA

A doença mental tem chamado a atenção do homem desde os tempos mais remotos. No início, a interpretação dada a ela tinha um cunho mágico-místico, acreditando-se que o doente mental estava possuído por algum espírito maligno. Na Roma Antiga, utilizavam-se, para os doentes mentais, os termos "furioso" e "mentecapto". O primeiro designava aquele que possui o espírito em fúria e o segundo, o que tem a mente (*menti)* aprisionada (*captus)*. Também era utilizado o termo energúmeno, que deriva do grego *energoúmenos,* significando aquele que está possuído pelo espírito do Mal Com esse entendimento, chega-se à era cristã, em que se apregoava como tratamentos eficazes para os doentes mentais o exorcismo ou sua queima nas fogueiras da Santa Inquisição (Palomba, 2003, p.03).

Ocorre que, como lembra Foucault (1978, p.64), com o advento da Renascença Européia, a miséria e a escória humana foram retiradas da esfera sagrada do misticismo cristão; e, assim, o internamento dos alienados passou

a representar o novo modo de o homem lidar com o que havia de inumano e desconhecido em sua existência. Assim, antes de assumir o sentido médico que hoje lhe atribuímos, o internamento iniciado na idade média teve razões iniciais que em nada se coadunavam com o objetivo de curar os enfermos, mas sim com o propósito de excluí-los e isolá-los (Foucault, 1978, pp.72-73).

Destarte, as primeiras ideias efetivamente científicas que buscaram desmistificar o tema da doença mental surgem com o médico holandês Johann Weyer, que, em 1563, publicou o livro *De praestigiis daemonum,* traduzido como *Da ilusão dos demônios*, no qual afirmou categoricamente que as doenças mentais são de origem natural e perfeitamente explicáveis pela Medicina, nada tendo a ver com práticas sobrenaturais (Palomba, 2003, p.06). Entretanto, o tratamento inicial dado à tais enfermidades não era dos mais humanos e, provocou durante muito tempo espanto e revolta por parte dos "alienados" e de seus familiares.

Contudo, há de se ter em mente que doenças de cunho psíquico não se confundem com doenças orgânicas, apesar de, muitas vezes, possuírem causas orgânicas e genéticas. Tais diferenças são apontadas sobretudo quando do diagnóstico e tratamento das mesmas. Michel Foucault (1975, p.11-14) especifica os principais pontos de divergência entre os mencionados tipos de doenças: primeiramente as doenças possuem abstrações diferentes; enquanto as doenças orgânicas e tratadas pela medicina encontram na própria fisiologia do indivíduo caminhos e formas de delimitação concreta; a psicologia não possui esse aporte nem mesmo na psiquiatria, sendo muito difícil delimitar o distúrbio e a extensão do seu dano ao conjunto da personalidade. Como segundo ponto, mas em decorrência do primeiro, vê-se que a medicina delimita com mais precisão as fronteiras do normal e do patológico, sabendo, portanto, quando deve ou não intervir; já para a psiquiatria é muito difícil definir quais aspectos da personalidade são normais ou indicam patologia. Por fim, as relações dos indivíduos organicamente adoentados e dos psicologicamente perturbados com o meio que os cerca também é muito distinta, já que este último possui um problema internalizado e, muitas vezes, imperceptível.

Foucault também ressalta que diante de um quadro de doença mental, vem em mente a ideia de um vazio funcional, pois a consciência daquela pessoa está enfraquecida. Segundo Foucault (1975, p.16), a imagem da doença mental remete à: "incapacidade de um sujeito confuso de se localizar no tempo e espaço, as rupturas de continuidade que se reproduzem incessantemente na sua conduta, a incapacidade de superar o instante no qual está enclausurado para atingir o universo do outro, ou para voltar-se para passado e futuro (...)". Entretanto, há um outro lado da moeda, pois este aparente vazio emocional em muitos casos é preenchido por novos tipos de reações e condutas que, muitas vezes podem ser exageradas e, até mesmo, descambar para a violência

e para a delinquência (Foucault, 1975, p.16). É com o lado ativo, portanto, da doença mental, que o Direito Criminal vai se preocupar.

3. A DOENÇA E AS ALTERAÇÕES MENTAIS À LUZ DO DIREITO PENAL

O ponto de encontro entre o Direito e a Psicanálise reside em saber como o sujeito subjetiviza a lei. O sujeito deve implicar-se subjetivamente em seu ato (estabelecer um debate consigo mesmo e com a lei). Quando um sujeito pratica um fato, não se pode esquecer a sua subjetividade (condições psíquicas e espirituais). Só é possível vincular o sujeito do ato ao ato criminal se a culpabilidade for acompanhada de responsabilidade, isto é, se o sujeito tiver a capacidade de subjetivar a culpa e atribuir uma significação ao seu ato. Para a Psicanálise, compreender o caráter ilícito do fato significa que o sujeito dá alguma significação a esse ilícito, que se envolve ética e moralmente em seu ato, ou seja, se reconheça como responsável (Rodrigues, 2019).

Já no contexto do Direito Criminal, quando se trata de doença mental, necessariamente há de se falar, em imputabilidade. A imputabilidade é a capacidade de culpabilidade, isto é, a aptidão para ser declarado culpável. A responsabilidade penal não se confunde com a imputabilidade: a responsabilidade penal significa que a pessoa dotada de capacidade de culpabilidade deve responder por seus atos; a imputabilidade, por sua vez, é um elemento da culpabilidade.

No Brasil, o Código Penal utiliza as seguintes expressões que remetem à nomenclatura médica psiquiátrica: *doença mental*, *desenvolvimento mental retardado*, *desenvolvimento mental incompleto* e *perturbação da saúde mental.* Vale lembrar que a doença mental, o desenvolvimento incompleto e o retardado, quando deixam o agente inteiramente incapaz de entender o caráter ilícito do fato ou de determinar-se segundo esse entendimento, causam a inimputabilidade e, com ela, a isenção de pena. Já a perturbação da saúde mental e o desenvolvimento incompleto e retardado, quando causam ao agente apenas a diminuição no entendimento do caráter ilícito do fato ou em sua determinação quanto a ele, implicam diminuição de pena de um a dois terços ou aplicação de medida de segurança (sistema duplo binário).

Assim, podemos notar que a *perturbação da saúde mental* somente pode levar à semi-imputabilidade, enquanto *o desenvolvimento incompleto ou retardado* pode levar, dependendo do grau – se completo ou parcial –, à inimputabilidade ou à semi-imputabilidade. Com relação à sanidade mental, o agente, para que seja declarado inimputável, além de não ser mentalmente sadio ou não apresentar desenvolvimento mental completo, por motivo de doença ou de perturbação mental, deve manifestar, também, a consequência desse distúrbio,

qual seja a ausência de capacidade de discernir ou de aquilatar seus próprios atos e de compará-los com a ordem normal (normativa).

Ocorrem, portanto, dois momentos distintos: o agente não é capaz de avaliar o que faz e/ou então é incapaz de autodeterminar-se (agir) no momento do fato. Esses dois aspectos são indispensáveis para a análise da questão da anormalidade psíquica do agente. Existem assim, dois aspectos, um biológico (doença ou anormalidade propriamente dita) e um psicológico (capacidade de agir segundo o entendimento que possui). Para que se possa afirmar que o sujeito é incapaz, basta que ele não apresente um dos dois aspectos (entendimento ou autodeterminação). É de clareza quase ofuscante que, se o sujeito não possui o entendimento ou a capacidade de avaliar seus próprios atos (valorar sua conduta de acordo com a ordem jurídica), também, por via de consequência, não vai possuir a capacidade de autocontrole ou de autodeterminação. O indivíduo só controla aquilo que entende e que sabe ser o certo ou o errado.

O oposto, entretanto, não é verdadeiro: o sujeito pode ter a plena capacidade de entender o caráter ilícito do fato que está prestes a praticar, mas pode não ter domínio sobre esse ato (falta o autocontrole, a autodeterminação). Esse segundo elemento, como se verá no momento oportuno, é o que parece muitas vezes faltar ao psicopata, ao pedófilo e à indivíduos com outros tipos de transtornos. Eles sabem o que é o certo e o errado e até, pode-se dizer, possuem a capacidade genérica de autocontrole ou de autodeterminação, mas, no caso concreto, quando passam a ter contato com a situação que o coloca em relação direta com o fato (passagem à ação), não mais controlam os seus atos (Rodrigues, 2019).

Fato é que, ainda que o Direito Penal traga como resposta ao inimputável a possibilidade de "tratamento" através da aplicação de medida de segurança; tais medidas, por se concentrarem em tratamento ambulatorial e internação, na grande maioria das vezes não dão conta de resolver o problema. Assim, ou o paciente fica indefinidamente submetido a tais medidas (até cessar sua periculosidade), ou será liberado e fará parte dos alarmantes índices de reincidência.

Diante de tão alarmante cenário, faz-se necessário extravasar os muros do Direito e mesmo das ciências da mente e buscar respostas no campo da Ciência Tecnológica moderna. Teria ela alcançado meios para desestimular comportamentos criminosos?!

4. TREINANDO O COMPORTAMENTO CRIMINOSO: O NEUROFEEDBACK

De posse de tais informações, a solução proposta neste projeto para um possível tratamento das pessoas com transtornos mentais e a redução das taxas de reincidência criminal destes indivíduos, é inspirada no trabalho de diversos psiquiatras, psicólogos, neurologistas, tecnólogos e juristas que acreditam

ser possível a referida redução, caso haja a devida identificação do distúrbio psiquiátrico em questão; e uma reeducação da personalidade com propensão criminosa através do que há de mais moderno em termos de medicina neural: os treinamentos realizados através da técnica de neurofeedback.

Entre os anos de 1960 e 1970, descobriu-se a possibilidade de recondicionar e retreinar os padrões de ondas cerebrais; especialmente com os estudos de Kamya, considerado o pai do neurofeedback. As ondas cerebrais ocorrem em várias frequências, algumas mais frequentes e outras menos: delta, teta, alfa, beta e gama; e são medidas em hertz; sendo gama a mais alta e delta a mais baixa (Hammond, 2011, p.305).

Deve-se ter em conta que cada indivíduo possui diferentes alterações destas frequências em diferentes áreas cerebrais. Pessoas com transtornos de personalidade geralmente apresentam um excesso de ondas de baixa frequência. Quando há uma grande quantidade destas ondas na parte frontal do cérebro se torna difícil controlar a atenção, o comportamento e mesmo as emoções. O neurofeedback seria, então, uma tentativa de reeducar estas ondas cerebrais, aumentando sua frequência e possibilitando aos indivíduos maior controle de suas emoções e de seu comportamento.

Para o treinamento, que é realizado através de Eletroencefalograma (ECG), em regra são utilizados dois ou mais eletrodos no escalpo e mais um ou dois nas orelhas; todos conectados a uma espécie de capacete, popularmente conhecido como "Brain Master". Então, equipamentos eletrônicos de alta tecnologia fornecem, em tempo real, feedbacks instantâneos sobre a atividade das ondas cerebrais do indivíduo. Com feedback continuo, treinamento e pratica as ondas cerebrais saudáveis podem ser reeducadas na maioria dos indivíduos (Hammond, 2011, p.306).

A utilização do Brain Master para redirecionamento da personalidade criminosa, teria por base estudos de auto-regulação do cérebro através do mapeamento das frequencias mais baixas, potências baixas emitidas na região cortical - Slow Cortical potentials (SCPs)- pois, os estudos já realizados em psicopatas demonstram uma desregulação da atividade cortical liminar e evidencias de deficiência cortical funcional (Konicar et al, 2015, p.01).

A deficiência de controle comportamental e os altos níveis de agressividade estão relacionados com um ativação excessiva do sistema comportamental e sensitivo que recompensa ou pune as atitudes realizadas pelo indivíduo. As anormalidades mais frequentemente observadas no EEG de pessoas violentas e com comportamento antissocial demonstram um grande nível de baixas frequências, reveladores, inclusive, de disfunção prefrontal nos psicopatas. Assim, um corpo consistente de evidencias associa o comportamento criminoso a um funcionamento excessivo dos circuitos límbicos pre-frontais e da conexão estabelecida entre estas regiões (córtex prefrontal, córtex anterior singularmente ínsula e amígdala).

Os problemas cognitivos e comportamentais que atingem àqueles com trantornos antissociais, como baixo cálculo antecipatório das consequências de suas atitudes, auto-controle deficiente e dificuladade de formação de expectativas estáveis; são regulados pelos circuitos pré-frontais-límbicos e estão relacionados ao o desenvolvimento de baixas potências na superfície cortical (SCPs) (Konicar et al, 2015, p.01).

Os resultados desta regulação cerebral intensiva demonstram que pessoas que cometem crimes, impulsionados por fatores neurológicos, estão sim aptos a adquirir o controle de sua excitação cerebral nas áreas fronto-centrais do cérebro. Com a aplicação do SCP self-regulation training, observou-se redução da agressividade nestes indivíduos; da impulsividade e das tendências de desvio comportamental; assim como o aprimoramento do controle sobre suas ações e aumento da sensibilidade cortical para avaliar procedimentos de conduta considerados moral e legalmente errados. Este estudo demonstrou melhorias neurofisiológicos, comportamentais e subjetivas em vários psicopatas que cometeram delitos. E, pode representar uma nova base de tratamento neuro-biológico para este resistente e reincidente grupo criminal (Konicar, et al, 2015, p.01).

Quirk (1995) reportou uma redução do indicie de reincidência criminal em psicopatas a partir de uma combinação entre o treinamento de neurofeedback e biofeedback. Também com a utilização das técnicas de neurofeedback, Smith e Sams (2005) conseguiram demonstrar qualitativamente melhorias na atenção e no comportamento de jovens delinquentes. Além disso, como já mencionado, muitos estudos acerca do autocontrole cerebral demonstram que participantes saudáveis podem aprender a modificar sua atividade cortical a partir de treinamentos com base no neurofeedback.

Assim, ainda que incialmente de maneira experimental; são lanças luzes sobre novas possibilidades de reeducação do comportamento criminoso, seja ele precipitado por questões patológicas, sociais ou mesmo psicológicas. Ao perceber que a atual função ressocializadora da pena não tem trazido os resultados, há séculos, esperados; talvez seja chegado o momento de recorrer às alternativas disponibilizadas pelas novas tecnologias.

CONCLUSÕES

Crime e loucura é temática que tem se tornado objeto de estudo das mais diversas Ciências. Há muito se percebe que o Direito, ainda que seja autônomo, não dá conta de resolver sozinho tais problemáticas; necessitando, assim, do apoio de outras áreas do conhecimento e, até mesmo, das novas tecnologias. O Direito Penal pune o criminoso saudável ou aplica medida de segurança ao doente mental; mas como evitar que o comportamento criminoso se repita, eu um ou noutro caso?!

A partir do entendimento e aceitação de que o comportamento criminoso é um fenômeno multifatorial é possível entender a grave falha no sistema penal vicariante adotado no Brasil. "Tratar um indivíduo com patalogias e/ou transtornos mentais incuráveis é um processo insatisfatório do ponto de vista da reincidência; ao passo em que, esperar a ressocialização de indivíduos em celas pequenas, insalubres e sem investimentos em segurança e crescimento pessoal dos apenados não tem demonstrado nenhum resultado em termos de redução da violência ou da criminalidade.

No âmbito dos transtornos mentais e patologias, até o aparecimento do neurofeedback como tratamento potencial para o comportamento ilimitado, antissocial e violento era, praticamente impossível pensar numa solução a longo prazo. A pergunta a ser feita é se criminosos, saudáveis ou não, estão aptos a reaprender a controlar sua atividade cerebral através do neurofeedback; e mais ainda, se as características próprias das personalidades criminosas, como desinibição, agressividade e comportamento antissocial podem diminuir após o treinamento com neurofeedback (Konicar, et al, 2015, p.02).

Os cientistas acreditam que sim e, também apostam que a melhoria no autocontrole cortical irá estimular também a melhoria do sistema cerebral que processa os erros de conduta e atitudes; resultando em um aumento da sensibilidade a falhas cometidas pelo próprio indivíduo. Se os criminosos são seres com maior dificuldade de sensibilização e, por isso mesmo, com prejuízos de adaptação moral e mesmo legal; talvez estimular a sua sensibilidade seja justamente a resposta para iniciar um tratamento efetivo destes indivíduos; diminuindo as taxas de violência e de práticas criminosas reiteradas.

REFERÊNCIAS

DALY, Martin; WILSON, Margo. **Homicide**: Foundations of human behavior. Routledge. 1988.

FOUCAULT, Michel. **A história da loucura na idade clássica**. Tradução José Teixeira Coelho Neto. São Paulo: Editora Perspectiva, 1978.

_____. **Doença mental e psicologia**. Rio de Janeiro: Tempo Brasileiro, 1975.

HAMMOND, Corydon. What is neurofeedback: na update. **Journal of Neurotherapy**, 2011.

KONICAR, Lilian. Brain self-regulation in criminal psychopaths. **Scientific Reports**, 2015.

LINO, Denis. Criminal Profiling – **Perfil Criminal**: Análise do comportamento na investigação criminal. São Paulo: Juruá Editora, 2021.

LOMBROSO, Cesare. **O homem delinquente**; tradução Sebastião José Roque. São Paulo: ícone. 2013.

PALOMBA, Guido Arturo. **Tratado de psiquiatria forense civil e penal.** São Paulo: Atheneu, 2003.

PICOLOTTO, Patricia. A influência da desagregação familiar na criminalidade de apenados. **II Simpósio em Gestão Pública**. Santa Maria: UFSM- Universidade Federal de Santa Maria. 2017.

RAINE, Adrian. O crime biológico: implicações para a sociedade e para o sistema de justiça criminal. **Revista de Psiquiatria do Rio Grande do Sul**. Abr, 2008.

RODRIGUES, Alexandre Manuel Lopes. **Psicopatia e imputabilidade penal:** Justificação sob o enfoque jusfundamental e criminológico. São Paulo: Lumen Juris. 2019.

Capítulo 8

Metaverso: Principais Entraves no Avanço do Metaverso no Brasil

Sherllen Carvalho Moreira
Flávia Christiane de Alcântara Figueira

Apesar das muitas vantagens do uso do metaverso na área jurídica, conforme apresentado no meu artigo publicado pelo Instituto Silvio Meira em agosto de 2023, alguns desafios são significativos, tais como questões de segurança de dados que é crucial para proteger informações confidenciais; inlcusão digital para assegurar que todas as partes tenham acesso igualitário à tecnologia necessária para participar efetivamente dos processos jurídicos no metaverso e privacidade de dados confidenciais e informações sensíveis são frequentemente discutidos e compartilhados em processos legais, e garantir a proteção desses dados é essencial.

O uso do metaverso no campo jurídico suscita diversas questões legais e regulatórias que devem ser enfrentadas para assegurar a legitimidade e conformidade das atividades realizadas nesse ambiente. Por exemplo, determinar a jurisdição adequada para litígios e disputas que ocorrem no metaverso pode ser altamente complexo, especialmente quando envolve partes localizadas em diferentes regiões geográficas. Além disso, é crucial garantir a validade legal dos atos realizados no metaverso, como audiências virtuais e acordos digitais, para que sejam reconhecidos legalmente.

A adoção de novas tecnologias enfrenta frequentemente, resistência devido ao conservadorismo e à relutância em modificar práticas estabelecidas, o que pode resultar em certa resistência por parte de advogados, juízes e outros profissionais do direito em adotar novos métodos tecnológicos.

Implementar a tecnologia do Metaverso requer um investimento significativo de tempo, energia, uma conexão de internet robusta e recursos financeiros consideráveis. No contexto brasileiro, onde a infraestrutura tecnológica ainda é precária em alguns estados e cerca de 28% da população não possui

acesso à internet, conforme revelado pela pesquisa TIC Domicílios do Comitê Gestor da Internet (CGI.br), a adoção do Metaverso permanece distante para muitos brasileiros. A tecnologia enfrenta diversos desafios, incluindo o alto custo dos dispositivos necessários, a acessibilidade para estudantes, pessoas de baixa renda e idosos, além da preocupação com o potencial aumento da segregação social decorrente da sua implantação, especialmente porque visa se tornar a próxima geração da internet.

O Metaverso é um tema fascinante e complexo, assemelhando-se às discussões e previsões dos impactos da Internet década de 1990, quando a web se democratizou.

No Brasil, muitas pessoas ainda enfrentam desafios significativos para acessar a internet. De acordo com dados do Instituto Brasileiro de Geografia e Estatística (IBGE) de 2022, aproximadamente 6,4 milhões de brasileiros não tinham acesso à internet em suas residências. Entre os principais obstáculos estão a infraestrutura inadequada, especialmente em áreas remotas, dificuldades financeiras para pagar pelos serviços de conexão e falta de habilidades digitais, o que limita o acesso a serviços online e informações essenciais para muitas pessoas.

Para superar esses desafios, é essencial investir em infraestrutura de internet em todo o país e promover iniciativas que ampliem o acesso a serviços online e educação em habilidades digitais. Garantir um acesso equitativo à tecnologia é um desafio crucial, pois nem todos têm os recursos necessários para participar plenamente do metaverso.

Portanto, é fundamental estar preparado para enfrentar esses obstáculos, para tanto é necessário investimentos contínuos em tecnologia e capacitação profissional para utilizar as ferramentas disponíveis. Além disso, os tribunais devem adotar políticas de comunicação mais integradas e eficientes, visando proporcionar um acesso mais amplo à justiça e reduzir a burocracia.

Capítulo 9

Notas Acerca do Instituto do Investidor Anjo no Brasil

Diego Magno Moura de Moraes
Fabrício Vasconcelos de Oliveira

1. O QUE É UMA *STARTUP*?

No que tange ao termo *Startup*, de acordo com Reis (2018), fora utilizado na seara de entendimento que se busca com o presente estudo, pela primeira vez em abril de 1970, em uma publicação do *New York Times*, entretanto se acalorou com a crise das empresas "ponto-com" entre 1996 e 2001, quanto foi formada uma bolha especulativa caracterizada pela alta das ações das novas empresas de tecnologia da informação e comunicação alocadas no espaço da Internet.

A Bolha da Internet, como ficou comumente conhecida, adotou a utilização do termo startup, que até então apenas significava um grupo de pessoas trabalhando por uma ideia diferente e com potencial de fazer dinheiro. Além disso, *startup*, na etimologia da palavra, também sempre foi sinônimo de iniciar algo e colocá-lo em funcionamento.

Quando se busca uma conceituação para o termo *Startup*, é possível vislumbrar nos escritos pátrios e de ordem mundial sobre a temática que não se encontra uma uniformização sobre tal conceito, mas o que mais nos aproxima de um conceito padrão é que se trata de uma sociedade jovem com um modelo de negócios repetível e escalável, em um cenário de incertezas e soluções a serem desenvolvidas. Embora não se limite apenas a negócios digitais, uma *startup* necessita de inovação para não ser considerada uma empresa de modelo tradicional.

Existem algumas características que definem esse tipo de empresa que excluem negócios tradicionais. Elas são: modelo de negócio inovador, repetível e escalável em um cenário de incertezas.

Antes de tudo, o modelo de negócios é diferente de um plano de negócios, que foca em estratégias detalhadas para atingir metas, por exemplo. No

modelo de negócios, o foco não é necessariamente no produto, mas no valor e, consequentemente, na rentabilidade. Em outras palavras, como o seu negócio soluciona a dor do cliente de forma lucrativa.

Muitas vezes, o desafio do modelo de negócios de *startups* é criar algo inovador: ou adaptar um modelo de negócios para uma área onde não é comumente aplicado, ou criar um modelo totalmente novo.

Para um negócio ser repetível significa que ele é capaz de entregar o mesmo produto em escala potencialmente ilimitada. Dessa forma, não é viável muitas customizações ou adaptações, pois a meta é multiplicar. Já ser escalável significa crescer cada vez mais sem que isso influencie no modelo de negócios. Como resultado, um modelo de negócio repetível e escalável que tem um *fit* no mercado tem grandes chances de ser uma startup de sucesso.

No Brasil, o conceito de *startup* foi se maturando até ser tipificado pela lei complementar 182/21, denominada de marco legal das *startups*, a qual estabeleceu que são enquadradas como *startups* as organizações empresariais ou societárias, nascentes ou em operação recente, cuja atuação caracteriza-se pela inovação aplicada a modelo de negócios ou a produtos ou serviços ofertados.

Nesse sentido, criar uma *startup* é fugir do tradicional. Como procura ser disruptiva, dificilmente uma *startup* vai ter um manual de como ser bem-sucedida. Não há como afirmar se a ideia ou projeto de empresa irão realmente deslanchar. Dessa forma, o caminho a ser trilhado e os passos que o empreendedor deve tomar são minimamente incertos.

É justamente por esse ambiente, recorrente até que o modelo de negócios seja bem definido, que tanto se fala em investimento para *startups*. Sem capital de risco, é muito difícil persistir na busca por um modelo de negócios que comece a gerar retorno financeiro e se sustente. O ideal é o negócio sobreviver até a comprovação de que o modelo existe e sua receita comece a de fato crescer. Caso contrário, provavelmente será necessário "pivotar", até que o modelo de negócio se estabeleça ou até uma nova rodada de investimentos para que essa *startup* se torne uma empresa sustentável.

Uma forma de lidar melhor com esse cenário de incertezas é o produto mínimo viável, também conhecido como MVP. Ele tem o objetivo de validar uma solução e ajudar a entender o que o cliente realmente quer gastando o mínimo possível.

Consolidou-se, nesse sentido, a ideia de que as *startups* precisam atender a "dor", as necessidades específicas, de um cliente ou grupo de pessoas, para que ela seja promissora e passe a ser rentável. Assim, as *startups* podem ser divididas de várias formas, sendo que as principais são entre tipos de negócio ou nichos onde atuam. Em relação aos tipos de negócio, destacam-se 03:

a) B2B (Business to Business): em livre tradução, negócios para negócios, esse tipo de startup atende outras empresas ao invés do consumidor final diretamente;
b) B2C (Business to Consumer): negócios para consumidores, essa startup fornece um serviço para o consumidor final;
c) B2B2C (Business to Business to Consumer): negócios para empresas para consumidores, é utilizada quando uma empresa faz negócios com outra visando uma venda para o cliente final.

Já os nichos onde atuam variam de acordo com a área da empresa, como, por exemplo: mercado financeiro (*Fintech*), saúde e medicina (*Healthtech*), educação (*Edtech*), direito (*Lawtech*), dentre outros.

2. A LEGALIDADE DO INVESTIDOR ANJO NAS *STARTUPS*

A figura do investidor anjo surgiu no direito pátrio como um instrumento adicional de fomento às *startups*.

Foi originalmente regulado no artigo 61-A da Lei complementar n º 123/06 (incluído pela lei complementar n º 155/16) nos seguintes termos:

> **Art. 61**-A. Para incentivar as atividades de inovação e os investimentos produtivos, a sociedade enquadrada como microempresa ou empresa de pequeno porte, nos termos desta Lei Complementar, poderá admitir o aporte de capital, que não integrará o capital social da empresa.
> **§ 1º** As finalidades de fomento a inovação e investimentos produtivos deverão constar do contrato de participação, c om vigência não superior a sete anos.
> **§ 2º** O aporte de capital poderá ser realizado por pessoa física ou por pessoa jurídica, denominadas investidor-anjo.
> **§ 3º** A atividade constitutiva do objeto social é exercida unicamente por sócios regulares, em seu nome individual e sob sua exclusiva responsabilidade.
> **§ 4º** O investidor-anjo:
> **I** - não será considerado sócio nem terá qualquer direito a gerência ou voto na administração da empresa;
> **II** - não responderá por qualquer dívida da empresa, inclusive em recuperação judicial, não se aplicando a ele o art. 50 da Lei no 10.406, de 10 de janeiro de 2002 - Código Civil;
> **III** - será remunerado por seus aportes, nos termos do contrato de participação, pelo prazo máximo de cinco anos.
> **§ 5º** Para fins de enquadramento da socied ade como microempresa ou empresa de pequeno porte, os valores de capital aportado não são considerados receitas da sociedade.
> **§ 6º** Ao final de cada período, o investidor-anjo fará jus à remuneração correspondente aos resultados distribuídos, conforme contrato de participação,

> não superior a 50% (cinquenta por cento) dos lucros da sociedade enquadrada como microempresa ou emp resa de pequeno porte.
> **§ 7º** O investidor-anjo somente poderá exercer o direito de resgate depois de decorridos, no mínimo, dois anos do aporte de capital, ou prazo superior estabelecido no contrato de participação, e seus haveres serão pagos na forma do art. 1.031 da Lei no 10.406, de 10 de janeiro de 2002 - Código Civil, não podendo ultrapassar o valor investido devidamente corrigido.
> **§ 8º** O disposto no § 7o deste artigo não impede a transferência da titularidade do aporte para terceiros.
> **§ 9º** A transferência da titularidade do aporte para terceiro alheio à sociedade dependerá do consentimento dos sócios, salvo estipulação contratual expressa em contrário.
> **§ 10º** O Ministério da Fazenda poderá regulamentar a tributação sobre retirada do capital investido.

Posteriormente, a lei complementar nº 182, de 1º de junho de 2021 ("institui o marco legal das *startups* e do empreendedorismo inovador; e altera a Lei nº 6.404, de 15 de dezembro de 1976, e a Lei Complementar nº 123, de 14 de dezembro de 2006") conceituou investidor anjo em seu art. 2º, I como: "investidor-anjo: investidor que não é considerado sócio nem tem qualquer direito a gerência ou a voto na administração da empresa, não responde por qualquer obrigação da empresa e é remunerado por seus aportes".

Da leitura dos referidos dispositivos decorre que o investidor anjo é um investidor que não é considerado sócio nem tem qualquer direito a gerência ou a voto na administração da empresa, porém, terá direito a realizar aportes.

Clarividente que o contrato realizado entre *startup* e investidor anjo não é um contrato social, o investidor não é um sócio constituído da atividade empresarial. O investimento não constitui capital social e o investidor não pode ser responsabilizado por dívidas sociais. Senão vejamos o que dispõe a lei complementar 182/21 acerca do tema:

> Art. 8º O investidor que realizar o aporte de capital a que se refere o art. 5º desta Lei Complementar:
> I - não será considerado sócio ou acionista nem possuirá direito a gerência ou a voto na administração da empresa, conforme pactuação contratual;
> II - não responderá por qualquer dívida da empresa, inclusive em recuperação judicial, e a ele não se estenderá o disposto no art. 50 da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), no art. 855-A da Consolidação das Leis do Trabalho (CLT), aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943, nos arts. 124, 134 e 135 da Lei nº 5.172, de 25 de outubro de 1966 (Código Tributário Nacional), e em outras disposições atinentes à desconsideração da personalidade jurídica existentes na legislação vigente.
> Parágrafo único. As disposições do inciso II do caput deste artigo não se aplicam às hipóteses de dolo, de fraude ou de simulação com o envolvimento do investidor.

Assim, evidente que a ideia de investimento anjo é fomentar investimentos nas *startups*, ao mesmo tempo que "protegem" esses investidores durante esse inicial cenário de incerteza do sucesso das *startups*, os "blindando" das responsabilidades sociais, em caso de insucesso.

3. TIPOS DE CONTRATOS QUE PODEM SER UTILIZADOS COMO FORMA DE INVESTIMENTO EM *STARTUPS* E SUAS IMPLICAÇÕES

No que tange as formas de investimento anjo tipificadas e autorizadas pela legislação, que mantém a supra mencionada proteção aos investidores ao mesmo tempo que fomenta a atividade empresarial das startups, o artigo 5º, da lei complementar 182, de 1º de junho de 2021, elucida que:

> Art. 5º As startups poderão admitir aporte de capital por pessoa física ou jurídica, que poderá resultar ou não em participação no capital social da startup, a depender da modalidade de investimento escolhida pelas partes.
> § 1º Não será considerado como integrante do capital social da empresa o aporte realizado na startup por meio dos seguintes instrumentos:
> I - contrato de opção de subscrição de ações ou de quotas celebrado entre o investidor e a empresa;
> II - contrato de opção de compra de ações ou de quotas celebrado entre o investidor e os acionistas ou sócios da empresa;
> III - debênture conversível emitida pela empresa nos termos da Lei nº 6.404, de 15 de dezembro de 1976;
> IV - contrato de mútuo conversível em participação societária celebrado entre o investidor e a empresa;
> V - estruturação de sociedade em conta de participação celebrada entre o investidor e a empresa;
> VI - contrato de investimento-anjo na forma da Lei Complementar nº 123, de 14 de dezembro 2006; (...)

Inicialmente, conforme a legislação vigente, um contrato que poderá ser utilizado para regular a relação entre investidor e *startup* é um contrato de participação negocial, através do qual o investidor realiza aportes financeiros no empreendimento do investido e negocia a expectativa de receber o referido valor em retorno, com acréscimo de remuneração sobre aquele valor.

Não se trata de contrato atípico vez que passou a existir previsão na lei complementar nº 123/06, sendo que a referida lei complementar se omitiu ao tratar a formar de tributação deste contrato de participação, se tornando algo turvo e que ainda traz dúvidas e riscos quanto a sua realização.

Ademais, conforme alhures exposto, também, vem sendo exploradas outras modalidades de contrato a serem realizados para a finalidade investidor anjo, que merecem atenção.

Alguns optam por firmar contrato de mútuo. O mútuo é previsto no art. 586 e seguintes do código civil e traz a possibilidade de uma pessoa física ou jurídica emprestar à outra, também física ou jurídica, coisa fungível, podendo, ainda, exigir juros quando da restituição do valor, sem que ultrapasse o limite legal. Viu-se vantagem em realizar tal contrato pois os impostos se limitavam ao IOF, que não tem grande impacto. O grande problema, que gera o desinteresse de alguns, é que o retorno se daria, necessariamente, pela taxa de juros aplicável ao valor emprestado.

A sociedade em conta de participação também tem sido muito utilizada para a realização do investimento anjo. Tal tipo societário é previsto nos arts. 991 e seguintes do CC. Neste instituto encontramos a figura do sócio ostensivo (que realiza a atividade empresarial diretamente com terceiros) e do sócio participante, também chamado de oculto que da aporte financeiro ao ostensivo, porem sem fazer parte do contrato social da atividade empresária.

Diferente do Mútuo, aqui não existem limites para a remuneração do sócio oculto, sendo pactuado em comum acordo no contrato celebrado entre as partes. O principal risco que se pode elencar é a responsabilização do investidor por débitos trabalhistas que surjam em nome do investido.

Outros contratos evidenciados pela legislação, partem para cenários relacionados aos títulos emitidos pelas sociedades, quais sejam, os contratos de subscrição ou compra de ações ou quotas e o contrato de conversibilidade de debentures, todos permitindo que inicialmente os investidores não adentrem no quadro societário, até que sintam segurança para tal, os protegendo em caso de fracasso da investida.

Nesse diapasão, encontramos várias formas contratuais de se formalizar a relação entre investidor anjo e *startups,* quais sejam, todos com caraterísticas adequadas, mas cada um com um ônus diferente ao investidor

4. RESPONSABILIDADE DOS INVESTIDORES

A maior preocupação dos investidores anjo é quanto a responsabilidade que podem ter perante a esfera civil e principalmente trabalhista em relação a dívidas da *startup*. Nesse contexto como já visto, a legislação de fato protege a figura do investidor anjo quando este realiza o contrato típico da lei complementar n º 123/06, que é o contrato de participação do 61-A, o qual não pode ser responsabilizado, porém caso o investidor opte por outra forma de contratação como a conta de participação, a comandita simples esse risco passa a ser considerado, em situações que a própria startup sentindo-se prejudicada por algum dano, cobrar o investidor. Correndo ainda o remoto risco, (caso preenchidos os requisitos do 50 do CC) da desconsideração da personalidade jurídica.

Mesma sorte tange a responsabilidade trabalhista ao investidor anjo, se celebrar um contrato baseado na participação da lei complementar n º 123/06, como não possuiria direitos na administração da *startup* não sofreria responsabilidade já no caso de optar pelas outras modalidades como conta de participação ou converter ou até adquirir quotas ou ações virando sócio, passaria a estar exposto ao risco, principalmente porque a seara trabalhista costuma utilizar a teoria menor para desconsiderar a personalidade jurídica.

Também podemos seguir a mesma linha de raciocínio para os débitos tributários, onde pelo contrato de participação não teriam a possibilidade de serem responsabilizados, nos demais casos a responsabilidade passaria a existir em caso de violação do art. 50 do CC.

5. A TRIBUTAÇÃO DO INVESTIDOR ANJO.

A tributação variará de acordo com a forma de contratação escolhida.

Se a opção for pelo contrato de parceria, deve ser obedecido disposto na Instrução Normativa n º 1719/2017 da Receita Federal, segundo a qual os rendimentos oriundos do contrato de parceria criado pela lei complementar n º 123/06 serão tributados pelo imposto de renda a alíquotas equivalentes àquelas exigidas das pessoas físicas, variando entre 15% e 22,5%. A referida Instrução ainda determina que os "lucros" auferidos em razão da transferência dos direitos creditórios do contrato de parceria a terceiros, permissivo expresso na Lei Complementar 123, também sofrerão tributação pelo imposto de renda na mesma modelagem.

No que diz respeito ao contrato de mútuo, a tributação é definida pela Instrução Normativa nº 1585/201528 da Receita Federal do Brasil que, em seus artigos 47 e 53 define ser tributável o rendimento auferido pelo mutuante (quem empresta) pelo imposto de renda.

O rendimento oriundo do mútuo também sofre tributação pelo IOF (imposto sobre operações financeiras), por força dos artigos 1º e 3º, §3º, III do Decreto 6306/2007. Portanto, a realização de contrato de mútuo como forma de gerir a relação entre investidor e investido parece fadada ao ostracismo, já seus rendimentos são limitados e, não obstante, pesadamente tributados.

Quanto à tributação da sociedade em conta de participação, como possui característica de mero contrato, de fato, não há criação de tributação específica.

Convencionou-se no meio contábil que a tributação das receitas do contrato de participação acompanhe a tributação do sócio ostensivo, na verdade, mais que isso, convencionou-se que a tributação será a mesma do sócio ostensivo, inclusive declarada pelo mesmo.

Portanto, como visto nas opções do contrato de parceria da lei complementar n º 123/06 e do contrato de mútuo já se explicou que incidirão impostos equivalentes às alíquotas de pessoas físicas sobre os rendimentos auferidos, no caso de opção pela sociedade em conta de participação as alíquotas incidentes sobre os rendimentos da parceria serão aquelas mesmas do sócio ostensivo (pessoa jurídica), portanto, no caso de micro e pequena empresa, alíquotas entre 4,5 e 16%.

REFERÊNCIAS

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.

BRASIL. Lei Complementar 123 de 14 de dezembro de 2006. **Diário Oficial da União**: seção 1, Brasília, DF, p. 1, 15 dez. 2006.

BRASIL. Lei Complementar 182 de 01 de junho de 2021. **Diário Oficial da União**: seção 1, Brasília, DF, p. 1, 01 jun. 2021.

REIS, Edgar Vidigal de Andrade. Startups: análise de estruturas societárias e de investimento no Brasil, São Paulo, Almedina, 2018.

Capítulo 10

O Impacto Positivo do Uso da Inteligência Artificial na Automação de Processos da Administração Pública

Rafaella Brandão Sousa Pinheiro

1. INTRODUÇÃO

A sociedade digital perpassa por inúmeras mudanças de acordo com os avanços tecnológicos e a inerência natural do ser humano em buscar a constante otimização de suas atividades resultou nos estudos científicos e criação da Inteligência Artificial (IA). A IA, definida como a capacidade de máquinas executarem tarefas que normalmente requerem inteligência humana, como reconhecimento de padrões, aprendizado e tomada de decisões, tem se consolidado como uma das mais promissoras estratégias para a modernização e eficiência da gestão de processos na Administração Pública.

Uma das áreas mais impactadas pela IA é a automação de processos administrativos. De acordo com Pinheiro (2022), a utilização de algoritmos de IA permite a análise rápida e precisa de grandes volumes de dados, facilitando a identificação de padrões e anomalias que podem informar políticas públicas mais eficazes. Além disso, a automação de processos por IA pode reduzir significativamente o tempo e os recursos necessários para executar tarefas administrativas, como o processamento de documentos e a gestão de recursos humanos.

No contexto brasileiro, a Estratégia Brasileira de Inteligência Artificial (EBIA) tem promovido o uso de IA na Administração Pública, com iniciativas que visam integrar essas tecnologias de forma ética e eficiente. A EBIA destaca a importância de garantir que a aplicação da IA respeite princípios de transparência, responsabilidade e segurança. O Projeto de Lei 2338/2023, atualmente em tramitação, também busca estabelecer um marco regulatório robusto para o uso de IA no Brasil, abordando aspectos como a proteção de dados e a responsabilidade pelos resultados gerados por sistemas de IA.

A proposta deste artigo é analisar o impacto positivo do uso da IA na automação da gestão de processos na administração pública brasileira, destacando os benefícios dessa transformação. A metodologia empregada para alcançar os objetivos deste estudo é a revisão sistemática da literatura, escolhida devido à sua capacidade de fornecer uma visão abrangente e estruturada sobre um campo de estudo específico, no caso, a intersecção entre inteligência artificial e gestão pública. Serão abordados no presente artigo o impacto das novas tecnologias no âmbito da administração pública, exemplos práticos de implementação da IA na esfera executiva, bem como a regulamentação necessária para garantir o uso ético e eficaz dessas tecnologias e a proposta de utilização da Inteligência Artificial na otimização de operações na PRODEPA. Assim, espera-se contribuir para a compreensão dos potenciais da IA na modernização da administração pública, promovendo um debate fundamentado sobre o futuro digital da gestão pública no Brasil.

2. O QUE É A INTELIGÊNCIA ARTIFICIAL?

A Inteligência Artificial - IA (Sigla da expressão *Artificial Intelligence*), é um campo da ciência da computação dedicado ao desenvolvimento de sistemas que possam realizar tarefas que normalmente requerem inteligência humana, como reconhecimento de fala e tomada de decisão. Pinheiro (2018) contextualiza que em nossa Era, a Tecnologia que desponta de modo disruptivo é a Inteligência Artificial, em especial o aprendizado de máquina (*machine learning*). O *software* consegue "aprender" pela experiência, melhora o seu desempenho sem a necessidade de humanos programarem explicitamente suas atividades. Segundo Pinheiro (2018), a IA envolve a criação de algoritmos e modelos computacionais capazes de simular processos cognitivos humanos. Dessa forma, a IA não apenas replica comportamentos humanos, mas também busca melhorar a eficiência e precisão desses processos.

Para Ludermir (2021), a IA é dividida em três diferentes subáreas, de acordo com as funções que é capaz de desempenhar. Os principais tipos de Inteligência Artificial são: A "IA Focada", também conhecida como "IA Fraca", consiste em algoritmos especializados em resolver problemas em uma área e/ou um problema específico – é a que mais usamos; a "IA Generalizada", também conhecida como IA Forte, os algoritmos desenvolvidos se tornam tão capazes quanto humanos em várias tarefas e utilizam técnicas de Aprendizado de Máquina (*machine learning*) como ferramenta - o nível atual da IA é de IA Generalizada; e a Superinteligência, ou ASI, que ainda se encontra em fase de estudos e promete revolucionar o nosso cotidiano.

3. HISTÓRIA DA INTELIGÊNCIA ARTIFICIAL

A história da inteligência artificial é marcada por várias fases de desenvolvimento e desafios. No Brasil, o interesse pela IA começou a ganhar força nas décadas de 1970 a 1990, com a criação de grupos de pesquisa e o desenvolvimento de sistemas especialistas (Milagre, 2023). No entanto, foi apenas no século XXI, com o avanço das tecnologias de processamento e armazenamento de dados, que a IA começou a se consolidar como uma área de pesquisa robusta.

Segundo Moreira, Melo & Martins (2020), em âmbito global, a IA começou a tomar forma na década de 1950, com os trabalhos pioneiros de Alan Turing e a conferência de *Dartmouth*, onde o termo "inteligência artificial" foi assinalado por John McCarthy. Turing, reconhecido por seu trabalho pioneiro na decodificação de mensagens alemãs durante a Segunda Guerra Mundial, avançou no campo da IA com a publicação de *"Computing Machinery and Intelligence"*. A Inteligência Artificial passou por períodos de grande otimismo, como nas décadas de 1960 e 1980, seguidos por fases de decepção, conhecidas como "invernos da IA". Esses períodos de baixa atividade foram causados por limitações tecnológicas e pela complexidade dos problemas que os sistemas de IA tentavam resolver (MOREIRA, MELO & MARTINS, 2020).

Nos últimos anos, o campo da IA vem ressurgindo notavelmente, impulsionado por avanços em aprendizado profundo (*deep learning*) e o aumento da disponibilidade de grandes volumes de dados (*big data*). No Brasil, este renascimento tem sido acompanhado por investimentos em pesquisa e desenvolvimento, tanto no setor público quanto no privado, e pela criação de centros de excelência em IA em universidades e instituições de pesquisa como o PRAIA Educação – Pesquisa Realmente Aplicada em Inteligência Artificial da Universidade Federal de Pernambuco (UFPE) e o CEREIA – Centro de Referência em Inteligência Artificial da Universidade Federal do Ceará (UFC) (BRASIL, 2024).

4. REGULAMENTAÇÃO DA INTELIGÊNCIA ARTIFICIAL NO BRASIL

Ainda não existe uma lei no Brasil que define o uso da Inteligência Artificial, mas como a evolução tecnológica é mais ágil do que o Legislativo para criação de leis, a IA já é utilizada no país mesmo sem regulamentação (PINHEIRO, 2022). Os debates regulatórios sobre a IA vêm ganhando força desde o ano de 2020, com a propositura do Projeto de Lei nº 21/2020, que não perdurou pela discrepância de arcabouço que permitisse a proteção e fiscalização con-

creta. Atualmente, um novo Projeto de Lei está em tramitação no Congresso Nacional, o PL 2.338/2023 que estipula normas gerais de caráter nacional para o desenvolvimento, implementação e uso responsável de sistemas de IA no Brasil (COALIZAÇÃO DIREITOS NA REDE, 2023).

A Estratégia Brasileira de Inteligência Artificial (EBIA), lançada em 2021, representa um marco importante nessa trajetória, a EBIA tem como objetivo promover a inovação e a competitividade da IA no Brasil, ao mesmo tempo em que assegura a proteção dos direitos humanos e a privacidade dos dados. Nesse cenário, ressalta-se como ponto primeiro positivo a preocupação com o desenvolvimento de uma IA responsável e protetiva aos direitos fundamentais.

Segundo Figueira (2023), uma regulamentação adequada e a consideração de princípios éticos são fundamentais para garantir que a Inteligência Artificial (IA) seja utilizada de forma responsável e em conformidade com os valores essenciais da sociedade. A Emenda Constitucional nº 115/2020 reforça a proteção de dados pessoais como um direito fundamental entre as garantias e os direitos fundamentais. A Lei Geral de Proteção de Dados (LGPD), vigente desde 2020, também desempenha um papel crucial na regulamentação da IA no Brasil. Ela estabelece um marco legal para o tratamento de dados pessoais, impondo requisitos rigorosos para a coleta, armazenamento e uso dessas informações.

4.1. Projeto de Lei 2.338/2023

O Projeto de Lei mais atual é o PL 2.338/2023, de autoria do senador Rodrigo Pacheco (PSD-MG), presidente do Senado Federal, está em tramitação no Congresso Nacional e surgiu como um marco significativo na trajetória de regulação da IA no Brasil, com o objetivo de proteger direitos fundamentais e garantir a implementação de sistemas seguros e confiáveis, em benefício da pessoa humana, do regime democrático e do desenvolvimento científico e tecnológico (ANPD, 2023).

Os principais pontos abordados no PL nº 2.338/2023, incluem: Definição e Classificação, definir o que é IA e estabelecer categorias baseadas na complexidade dos sistemas; Princípios e Diretrizes, estabelecer princípios éticos; Responsabilidade Civil, determinar as responsabilidades de desenvolvedores, operadores e usuários de IA; a Supervisão e Fiscalização, criar órgãos de monitoramento da IA; e Segurança e Privacidade, definir medidas para proteger dados pessoais e garantir a segurança cibernética (ANPD, 2023). Para Pinheiro (2018), a regulamentação deve focar em princípios como transparência, explicabilidade, e auditabilidade, para que os sistemas de IA possam ser compreendidos e monitorados adequadamente.

5. IMPACTO DAS NOVAS TECNOLOGIAS NA ADMINISTRAÇÃO PÚBLICA

A adoção de tecnologias digitais na administração pública tem potencializado a prestação de serviços de maneira mais eficiente e transparente. Os avanços tecnológicos encontram seu espaço certo quando bem dimensionados e estruturados, assim tornam-se grandes alavancadores nas boas práticas da gestão pública (GARCIA, 2011).

Em tempos de indústria 4.0, um novo tipo de Administração está despontando, e não há dúvida de que o modelo gerencial é mais eficiente do que os modelos burocráticos, em virtude da transformação digital que vem sendo impulsionada pela adoção de tecnologias emergentes, como Inteligência Artificial (IA) e *big data*. (LEITÃO & FERREIRA, 2021). A IA é uma das tecnologias emergentes que têm maior potencial para transformar a administração pública. No Brasil, a implementação de sistemas de IA nos Tribunais já é uma realidade efetiva e de exímios resultados, na gestão pública tem sido objeto de estudos e já está sendo executada em alguns estados.

5.1. IA na Administração Pública: O Caso da ALICE do TCU

Um exemplo emblemático de uso de IA na administração pública brasileira é a ALICE (Análise de Licitações e Editais), desenvolvida pelo Tribunal de Contas da União (TCU). A ALICE é uma ferramenta de análise automatizada que utiliza IA para examinar processos de licitação e contratos administrativos, identificando possíveis irregularidades e fraudes de forma rápida e precisa.

Segundo o TCU (2024), a ALICE foi treinada com milhões de dados históricos de processos de licitação, o que lhe permite identificar padrões e anomalias que poderiam passar despercebidos por análises humanas. A implementação dessa ferramenta resultou em um aumento significativo na eficiência das auditorias do TCU, reduzindo o tempo necessário para a análise de processos complexos e aumentando a detecção de irregularidades.

A ALICE exemplifica como a IA pode ser utilizada para melhorar a governança e a transparência na administração pública. Ao automatizar tarefas repetitivas e complexas, a IA libera os auditores para focar em questões mais estratégicas, contribuindo para uma gestão pública mais eficaz e responsável.

5.2. Outra Aplicação de IA no Executivo: A 1ª Secretaria de Inteligência Artificial do Brasil

A aplicação de IA nas prefeituras brasileiras é um exemplo notável de como essas tecnologias podem transformar a administração pública. Curitiba,

por exemplo, foi pioneira ao criar a primeira Secretaria de Inteligência Artificial do Brasil em 2024. Essa secretaria visa integrar a IA na gestão municipal para melhorar a eficiência dos serviços prestados aos cidadãos e apoiar a inovação na cidade (CURITIBA, 2024).

Curitiba, já utiliza a IA em soluções que dinamizam o serviço público, como a Central 156 de Atendimento ao Cidadão, que usa sistemas baseados em *chatbots*, assistentes virtuais, reconhecimento de voz e de imagem, que fornecem informações e serviços; o Zeladoria Digital foi desenvolvido um sistema que emprega inteligência virtual embarcada em veículos para analisar e processar dados das ruas, indicando aos gestores públicos onde são necessárias melhorias; e o CPPGM – Controle de Processos da Procuradoria-Geral da Prefeitura de Curitiba, que é um sistema de controle, peticionamento e o acompanhamento dos processos judiciais a partir de automatização e a padronização de tarefas repetitivas com o uso da IA.

6. UMA PROPOSIÇÃO DA UTILIZAÇÃO DA IA NA PRODEPA

A transformação digital na administração pública envolve a integração de Tecnologias da Informação e Comunicação (TIC) para modernizar processos e serviços (PINHEIRO, 2022). No contexto paraense, a Empresa de Tecnologia da Informação e Comunicação do Estado do Pará (PRODEPA), a qual é uma TIC, desempenha um papel crucial na implementação de soluções tecnológicas inovadoras para melhorar a gestão pública. O presente tópico abordará os benefícios dessa implementação, as melhorias e eficiência dos serviços com a proposição da IA.

6.1. Eficiência Operacional

A implementação da IA na PRODEPA pode aumentar consideravelmente a eficiência operacional. A automatização de processos administrativos reduz o tempo de execução de tarefas rotineiras, permitindo que os servidores públicos se concentrem em atividades estratégicas. A IA pode automatizar a triagem de documentos, a análise de dados e a resposta a consultas de cidadãos, resultando em um uso mais eficiente dos recursos humanos e financeiros (PINHEIRO, 2022).

6.2. Transparência e Governança

A transparência é um dos pilares da boa governança pública. A IA pode ajudar a PRODEPA a monitorar e auditar processos de forma contínua e detalhada. A utilização de algoritmos para auditar transações e processos pode

detectar inconsistências e irregularidades, promovendo a responsabilidade e a transparência (MENENGOLA, 2021). No contexto paraense, a aplicação de IA pode aumentar a confiança do público na gestão pública, ao assegurar que os processos sejam conduzidos de maneira íntegra e transparente.

6.3. Tomada de Decisão Baseada em Dados

A IA pode fornecer *insights* valiosos para a tomada de decisão na PRODEPA. A análise de grandes volumes de dados (big data) permite identificar padrões e tendências que informam a formulação de políticas públicas mais eficazes (JÚNIOR; BARBOSA; RODRIGUES, 2022). No Pará, a PRODEPA pode utilizar IA para analisar dados de diferentes fontes, como saúde, educação e segurança, melhorando a alocação de recursos e a resposta a necessidades emergentes.

6.4. Inovação e Competitividade

A adoção de IA na PRODEPA pode posicionar o Estado do Pará como um líder em inovação tecnológica no setor público. A implementação de tecnologias emergentes como a IA pode atrair investimentos e talentos, fomentando um ecossistema de inovação (MENENGOLA, 2021). A PRODEPA, ao liderar essa transformação, pode servir de modelo para outras entidades públicas no Brasil, demonstrando o potencial da tecnologia para revolucionar a gestão pública.

CONCLUSÃO

O uso de Inteligência Artificial (IA) na gestão de processos administrativos na Administração Pública representa um avanço significativo em termos de eficiência, transparência e inovação. A implementação de tecnologias de IA, como exemplificado pela ALICE do TCU e pela Secretaria de Inteligência Artificial de Curitiba, demonstra como estas ferramentas podem otimizar a análise de dados, reduzir a burocracia e promover uma governança mais eficaz.

A regulamentação da IA no Brasil, busca garantir que o desenvolvimento e a aplicação dessas tecnologias ocorram de forma ética e segura, respeitando os direitos fundamentais e a privacidade dos cidadãos. Estas iniciativas são essenciais para assegurar que a IA seja utilizada de maneira responsável, promovendo a confiança pública e a integridade dos processos administrativos.

A proposta de utilização da IA na PRODEPA ressalta os benefícios potenciais para a eficiência operacional, a transparência, a tomada de decisão baseada em dados, a inovação e a sustentabilidade. A implementação de IA pode

transformar a administração pública no Pará, posicionando o estado como um líder em inovação tecnológica no setor público e servindo de modelo para outras entidades no Brasil assim como exemplificado pela cidade de Curitiba, eleita em 2023 como a cidade mais inteligente do mundo.

Em suma, a incorporação da IA na esfera executiva não só moderniza a administração pública e gestão de processos, mas também contribui para a criação de um ambiente mais transparente, eficiente e orientado para o futuro. Ao promover a adoção responsável e regulamentada dessas tecnologias, o Brasil pode aproveitar plenamente o potencial da IA para melhorar os serviços públicos e a qualidade de vida dos cidadãos.

REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **NOTA TÉCNICA N° 16**: Sugestões de incidência legislativa em projetos de lei sobre a regulação da Inteligência Artificial no Brasil, com foco no PL nº 2338/2023. Brasil: CGTP, 2023. 13 p.

COALIZAÇÃO DIREITOS NA REDE. **NOTA TÉCNICA PROJETO DE LEI N° 2338/2023**: Nota Técnica sobre o Projeto de Lei 2.338/2023. Brasil: Lapin - Laboratório de Políticas Públicas e Internet, 2023. 13 p. Disponível em: https://direitosnarede.org.br/2023/08/23/coalizao-direitos-na-rede-divulga-nota-tecnica-sobre-o-pl-2338-2023-que-busca-regular-a-ia/. Acesso em: 20 jun. 2024.

CURITIBA, Prefeitura de (ed.). **Curitiba ganha a 1ª Secretaria de Inteligência Artificial do Brasil na abertura do Smart City Expo. 2021**. Disponível em: https://www.curitiba.pr.gov.br/noticias/curitiba-ganha-a-1-secretaria-de-inteligencia-artificial-do-brasil-na-abertura-do-smart-city-expo/72723. Acesso em: 20 jun. 2024.

FEDERAL, Governo. **Ministério anuncia mais quatro Centros de Pesquisa em Inteligência Artificial**. 2023. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/noticias/2023/09/ministerio-anuncia-mais-quatro-centros-de-pesquisa-em-inteligencia-artificial. Acesso em: 20 jun. 2024.

FIGUEIRA Flávia, 2023. **A Regulação da Inteligência Artificial e o Impacto nas Questões Éticas e Sociais.** São Paulo: USP, 2023. Disponível em: https://understandingai.iea.usp.br/wp-content/uploads/2023/09/A-Regulac%CC%A7a%CC%83o-da-Intelige%CC%82ncia-Artificial-e-o-Impacto-nas-Questo%CC%83es-E%CC%81ticas-e-Social-FINAL.pdf. Acesso em: 15 jun. 2024.

GARCIA, Fernando César Soares. **Inovações Tecnológicas na Administração Pública: estudo de caso do Serviço de Administração do Centro de Documentação e Informação da Câmara dos Deputados**. 2011. 65 f. Monografia (Especialização) - Curso de Gestão Pública Legislativa, Centro de Formação, Treinamento e Aperfeiçoamento da Câmara dos Deputados/Cefor, Brasília, 2011.

LEITÃO, Andre Studart; FERREIRA, Hélio Rios. As Novas Tecnologias a Serviço da Nova Administração: A Blockchain, os Smart Contracts e a Nova Lei de Licitações e Contratos (Lei nº 14.133/2021). **Revista de Direito Brasileira - RDB**, Brasil, v. 29, n. 11, p. 71-91, nov. 2021.

LUDERMIR, Teresa Bernarda. Inteligência Artificial e Aprendizado de Máquina: estado atual e tendências. **Estudos Avançados**, [S.L.], v. 35, n. 101, p. 85-94, abr. 2021. FapUNIFESP (SciELO). http://dx.doi.org/10.1590/s0103-4014.2021.35101.007.

MOREIRA, Luiz F. L.; MELO, Cláudio S.; MARTINS, Philippi H. **INTELIGÊNCIA ARTIFICIAL E BOAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO NO AMBIENTE CORPORATIVO.** 2023. 25 f. TCC (Graduação) - Curso de T.I e Computação, Unisul, Florianópolis, 2023. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/38672. Acesso em: 20 jun. 2024.

MENENGOLA, Everton J. F. **Blockchain no setor público brasileiro: a eficiência como fator fundamental para o desenvolvimento. Interesse Público** [Recurso Eletrônico]. Belo Horizonte, v.23, n.129, set./out. 2021. Disponível em: https://dspace.almg.gov.br/handle/11037/42341. Acesso em: 21 jun. 2024.

MILAGRES, Rafael. **A Evolução Da Inteligência Artificial No Brasil**. 2024. Milagre Digital. Disponível em: https://milagredigital.com/a-evolucao-da-inteligencia-artificial-no-brasil/. Acesso em: 20 jun. 2024.

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES SECRETARIA DE EMPREENDEDORISMO E INOVAÇÃO. **PORTARIA MCTI N° 4.979, DE 13 DE JULHO DE 2021**: Estratégia Brasileira de Inteligência Artificial. Brasília, 2021. 51 p.

PINHEIRO, Patricia. Capítulo I: Robotização, Inteligência Artificial e Disrupção In: PINHEIRO, Patricia. Direito Digital Aplicado 3.0. São Paulo (SP: Editora Revista dos Tribunais. 2018. Disponível em:https://www.jusbrasil.com.br/doutrina/secao/capitulo-i-robotizacao-inteligencia-artificial-e-disrupcao-direito-digital-aplicado-30/1197026358

PINHEIRO, Patrícia. **Direito Digital Aplicado 5.0**. São Paulo: Revista dos Tribunais, 2022. 336 p.

SILVA JÚNIOR, Enézio de Deus; BARBOSA, Gabriel Oliveira; RODRIGUES, Paulo Jorge Canas. Big data e políticas públicas. **Ba&D - Bahia Análise e Dados**, Salvador, v. 30, p. 7-12, dez. 2022. Disponível em: https://sei.ba.gov.br/images/publicacoes/download/aed/big_data.pdf. Acesso em: 30 jun. 2024.

TCU. BRASIL. Secom. TCU (org.). **Uso de inteligência artificial aprimora processos internos no Tribunal de Contas da União**. 2024. Disponível em: https://portal.tcu.gov.br/imprensa/noticias/uso-de-inteligencia-artificial-aprimora-processos-internos-no-tcu.htm. Acesso em: 15 jun. 2024.

Capítulo 11

O Papel do Direito Digital na Proteção das Vítimas de Violência Doméstica em um Mundo Tecnológico

Victor de Moura Carvalho Vallinoto

A violência doméstica é um grave problema que afeta milhões de pessoas em todo o mundo. Ela engloba uma variedade de comportamentos abusivos, físicos, emocionais, sexuais ou econômicos, que ocorrem dentro do ambiente familiar. Com o avanço da tecnologia e a presença cada vez maior da internet e das redes sociais em nossas vidas, a violência doméstica adquiriu novas dimensões, dando origem ao que chamamos de violência doméstica digital. Neste artigo, exploraremos a interseção entre a violência doméstica e o direito digital, e como esse campo emergente do direito pode proteger as vítimas nesse mundo conectado.

O QUE SERIA A VIOLÊNCIA DOMÉSTICA DIGITAL?

A violência doméstica digital é uma realidade e denomina-se como uma forma de abuso que ocorre através do uso de tecnologia, dentre eles, por telefones celulares, computadores, redes sociais, aplicativos de mensagens e e-mails. Isso inclui a disseminação de informações privadas sem consentimento, perseguição online, ameaças virtuais, assédio cibernético, controle coercitivo através do monitoramento constante e manipulação emocional.

O IMPACTO DA DESIGUALDADE SOCIAL E ECONÔMICA

O impacto da desigualdade social e econômica vem atingindo mais as mulheres durante a pandemia. A redução dos registros de lesões corporais e estupros no início da pandemia, longe de ser comemorada, nos manifesta a subnotificação desses crimes e a consequente dificuldade de acesso à Justiça por parte das mulheres, principalmente negras e indígenas. De acordo com

os dados nacionais, as mulheres não tiveram como denunciar a violência porque grande parte dos serviços estava funcionando parcialmente e, em alguns casos, apenas de forma digital, gerando obstáculo quase instransponível para as mulheres, sobretudo as que residem nas regiões mais afastadas dos centros urbanos, no campo e nas florestas.

Os dados nacionais apontam que houve aumento dos crimes de feminicídio durante a pandemia em cerca 22%, mas a violência letal não atinge as mulheres da mesma forma, porque a taxa de homicídios de mulheres negras foi de 5,2 por cem mil habitantes, enquanto a taxa de mulheres não negras foi de 2,8 %. Nesse sentido, o recorte de raça é fundamental para refletir sobre as desigualdades raciais e a ausência de políticas públicas para enfrentar o racismo estrutural e a violência contra as mulheres negras.

Num país com a crescente feminização da pobreza, as mulheres enfrentaram mais um desafio: os obstáculos para realizar uma denúncia de violência doméstica e familiar. O inimigo mora dentro de casa, a falta de acesso à internet, o medo do contágio pelo vírus e o de morrer por denunciar são as maiores causas da subnotificação.

A falta de acesso à educação durante a pandemia atingiu mais fortemente as crianças e os adolescentes das escolas públicas, que não têm como acompanhar as aulas remotas (quando há), seja por falta de acesso digital ou falta de acesso à internet, o que também tem impactado a vida das mulheres. Existe um verdadeiro abismo social entre alunos da rede privada e da rede pública de ensino. Os alunos da rede privada continuam com as aulas *online* nos seus computadores, no conforto das suas casas, e os alunos das comunidades, favelas e periferias estão sem aulas, e o pior, sem alternativas.

Isso também vem causando mais dificuldades para as mulheres, especialmente as vítimas que estão vivendo uma situação de violência doméstica, que não têm com quem, nem onde deixar os filhos para trabalhar e estudar. A falta de creches públicas e as escolas fechadas terão um impacto social e econômico enorme para o futuro do Brasil. Pobreza e desigualdade de gênero trarão serias consequências para o desenvolvimento humano do Brasil. A perda será irreparável e atitudes precisam ser tomadas pelos atuais governantes.

O estudo ainda aponta que existem desigualdades entre as várias regiões do Brasil. Dados do IBGE mostram que o menor índice de lares conectados à internet está no Nordeste, com 69,1%. Ou seja: mais de 30% das residências da região estão *offline*. Em relação à zona rural no país, o quadro é muito pior: menos de 50% das casas têm acesso à rede. No Norte, 77% das famílias fora da zona urbana estão desconectadas.

O acesso à internet foi incluído pelo Conselho dos Direitos Humanos da ONU como um direito humano, derivado da liberdade de expressão, comunicação e opinião. Isso porque se entende que a internet é uma ferramenta in-

dispensável para a realização da multiplicidade de direitos humanos, combate à desigualdade e aceleração do desenvolvimento.

Em relação à Justiça, temos de pensar na criação de políticas públicas judiciárias que sejam mais inclusivas e democráticas, que permitam às mulheres realizar as denúncias e acompanhar os seus processos judiciais sem burocracia, com acolhimento e respeitando os direitos humanos.

Exemplo de boa prática de acesso à Justiça recentemente lançada no Rio de Janeiro refere-se à criação do projeto Maria da Penha Virtual, um *app* em parceria entre o Tribunal de Justiça e a Universidade Federal do Rio de Janeiro – UFRJ, para que as mulheres vítimas de violência possam requerer diretamente a medida protetiva de urgência à Justiça, por qualquer meio eletrônico disponível, garantindo que a decisão judicial seja concedida em poucos minutos.

Um dos grandes desafios agora é democratizar o acesso à Justiça, com a criação de ferramentas mais acessíveis, e disponibilizar talvez centros de cidadania e Justiça para as mulheres que facilitem a inclusão digital, garantindo sobretudo às mulheres o direito de acesso à Justiça de forma irrestrita e igualitária e a viver uma vida livre de violência.

A IMPORTÂNCIA DO DIREITO DIGITAL NA PROTEÇÃO DAS VÍTIMAS

Legalmente, em nossa Legislação vigente, o direito digital desempenha um papel fundamental na criação e aplicação de leis específicas para combater a violência doméstica digital. É de suma importância, que os governos estabeleçam legislações abrangentes e eficazes para abordar essa forma de abuso, reconhecendo a gravidade das consequências emocionais, psicológicas e sociais que podem resultar dela.

O direito digital busca proteger a privacidade e a segurança das vítimas de violência doméstica, fornecendo mecanismos legais para que elas possam se proteger contra a exposição não autorizada de informações pessoais. Isso inclui ações legais contra a divulgação não consensual de imagens íntimas (pornografia de vingança) e a obtenção indevida de informações privadas.

As leis do direito digital podem estabelecer medidas para restringir a perseguição online, como a proibição de contatos indesejados, o bloqueio de contas de mídia social e a obtenção de ordens de restrição digital. Essas medidas ajudam a limitar o acesso do agressor à vítima e proporcionam um ambiente online mais seguro.

O direito digital também desempenha um papel crucial na conscientização e educação sobre a violência doméstica digital. É fundamental fornecer informações sobre os diferentes aspectos da violência doméstica online, bem como sobre os recursos disponíveis para as vítimas, incluindo linhas de apoio, organizações de suporte e agências governamentais especializadas.

AS FERRAMENTAS DIGITAIS NO COMBATE A VIOLÊNCIA DOMÉSTICA DIGITAL E OS PONTOS POSITIVOS

De acordo com o portal BID, brasileiras contam com a ferramenta PLP 2.0 desde 2015. Uma plataforma de utilidade pública de auxílio ao enfrentamento à violência doméstica que foi idealizada pelas organizações Geledès – Instituto da Mulher Negra e Themis – Gênero, Raça e Justiça com o objetivo fortalecer a rede de proteção para mulheres em situação de violência doméstica, entre todas, destacamos:

- O PLP 2.0 - esta ferramenta tem duas dimensões: a versão Juntas, que está disponibilizada para as mulheres em geral permitindo a todas construir a sua rede pessoal de proteção e a versão PLP2.0 que destina-se a mulheres com medidas protetivas permitindo a instantânea denúncia dos atos de violência e seu imediato encaminhamento às esferas de proteção e aplicação da (Lei nº 11.340/06 (LEI MARIA DA PENHA), o grande diferencial da ferramenta é permitir a articulação de uma rede de proteção que envolve entes públicos (polícia, delegacias, varas especializadas, Secretarias da Mulher, Ministério Público e (CNJ) e organizações da sociedade civil de defesa das mulheres, de direitos humanos e a rede de Promotoras Legais Populares (PLPs).
- ISA BOT - um robô criado pela organização Think Olga e pelo Mapa do Acolhimento, com o apoio de Facebook, Google e ONU Mulheres. A solução fornece orientações para meninas e mulheres em situação de violência, podendo ser acessada no chat do Google Assistente ou do Facebook.
- TODOS POR UMA - um aplicativo que permite o envio de avisos (pedidos de socorro) para contatos selecionados como "Anjo". Já foram realizados mais de 20 mil downloads da solução, que também está presente em países como EUA, Colômbia e Alemanha.
- O PROJETO GLÓRIA - que combina três tecnologias disruptivas – *blockchain*, inteligência artificial e *analytics* – para aprimorar a coleta, análise e disponibilização de dados relacionados à violência contra meninas e mulheres, possibilitando a construção de políticas públicas com base em evidências.
- FRIDA (A assistente virtual no combate à violência doméstica) - É uma assistente virtual que realiza atendimento imediato à vítima – acolhe a denúncia, esclarece dúvidas, faz uma avaliação preliminar do risco e aciona a polícia em situações de flagrante ou risco, inclusive enviando uma viatura. Além disso, faz uma triagem do que a vítima precisa, ofe-

recendo aconselhamentos e agendando uma horário para que a vítima vá até a delegacia fazer as medidas protetivas.

- SALVE MARIA - a ferramenta foi lançada em 28 de março de 2022 pela Secretaria de Estado da Mulher e dos Direitos Humanos (*Semudh*) em parceria com a Agência de Tecnologia da Informação (ATI) do Piauí. está disponível nas plataformas digitais para ser baixado. Ao acessar o dispositivo, as mulheres têm acesso ao botão do pânico, para ser acionado em caso de emergência, além da opção de enviar denúncias, que podem ser anônimas, sobre agressões (físicas, morais ou psicológicas), com detalhamento de informações, fotos e vídeos.

Além dessas plataformas digitais importantes, as rede sociais tem ajudado muito no combate a essa violência letal contra meninas e mulheres, bem como vídeos expostos nas redes sociais, tanto de agressões sofridas, como as audiências online que novamente vitimizam essas vítimas, diante a exposição e repercussão acabam tendo uma visibilidade de forma positiva, com a ajuda, clamor, compartilhamentos e cobrança da sociedade perante as autoridades.

ALGUNS EXEMPLOS DE CASOS EXPOSTOS NAS REDES SOCIAIS

- CASO DA MENINA DE 10 ANOS – a vítima estuprada pelo tio de 33 anos, em Recife (PE), O caso veio a público quando ela e a avó deram entrada no Hospital Roberto Silvares, no Espírito Santo, com mal-estar abdominal. O procedimento está assegurado pela Lei. A equipe médica desconfiou da barriga "crescida" da menina. Ao realizar exames, os enfermeiros descobriram que ela estava grávida de três meses. Em conversa com médicos, a criança confidenciou que o tio a estuprava desde os seis anos e que nunca contou aos familiares por que era ameaçada. O tio de 33 anos fugiu depois que a gravidez foi descoberta e tentou fugir, acabou sendo encontrado por tanta repercussão e exposição feita pela população nas redes sociais.
- CASO MARIANA FERRER - a vítima foi realocada à condição de culpada em plena audiência de instrução e julgamento do homem que supostamente a violou. Humilhada por agentes públicos que permitiram o achincalhamento de sua dignidade, ouviu comentários misóginos empregados em estrutura retórica presenciavam as agressões que se repetiam diariamente. O Caso repercutiu e gerou locomoção e a indignação da sociedade por meio das redes sociais.
- CASO SHANTAL - Vídeos e áudios foram expostos nas redes sociais de uma cruel Violência obstétrica que a vítima sofreu durante o parto

de sua filha, nos vídeos e áudios vazados, foram expostos vários xingamentos, palavrões e exposição da intimidade da vítima. Apenas depois de ter visto os vídeos foi que ambos, tanto o marido quanto a vítima perceberam que foi cruelmente violentada, além de áudios enviados pelo médico depois do ocorrido, relatando e repetindo os mesmo xingamentos contra o casal.

- CASO PAMELLA GOMES - a vítima Compartilhou uma série de vídeos que mostrava seu ex-marido Dj Ivis, agredindo de tapas, socos e chutes, na presença da filha e de outras pessoas que sempre voltada a justificar que se alguma violência Mariana sofreu. Ela foi revitalizada, e o tratamento a Mariana durante audiência virtual gerou indignação nas redes sociais depois da divulgação do vídeo.

STALKING

O termo que significa na língua inglesa "perseguição", está insertado no Código Penal Brasileiro, em seu artigo 147-A. O *stalking* pode enquadrar a violência doméstica digital por ser um ato de perseguição, pois as redes sociais servem de meio para que os infratores invadam as vidas da vítima com perfis falsos, ameaçando sua integridade moral, perturbando sua esfera de liberdade ou privacidade. A Lei 14.132/21 foi responsável por inserir no respectivo artigo acima mencionado, "o crime de perseguição", que tem sua finalidade na tutela da liberdade individual, abalada por condutas que constrangem alguém a ponto de invadir severamente sua privacidade e de impedir sua livre determinação e o exercício de liberdade básicas.

CONSIDERAÇÕES FINAIS

Entretanto faz com que se torne um meio muito positivo para o combate e o enfrentamento a essa violência para que não passe impune, visto que durante a pandemia as redes sociais se tornaram o principal meio de comunicação e vários casos foram expostos na mídia, então vem o questionamento e se não tivesse toda essa exposição? Ficaria impune? Provavelmente sim, devido a realidade que é a violência contra meninas e mulheres e como ainda essa situação tem como possível efeito colateral e consequências perversas para essas vítimas.

A violência doméstica digital é uma realidade preocupante nos dias de hoje, e o direito digital desempenha um papel vital na proteção das vítimas nesse contexto. É necessário desenvolver uma legislação adequada que reconheça a gravidade dessa forma de abuso e estabeleça medidas eficazes para combatê-la. Além disso, é essencial fornece recursos e suporte às vítimas, bem

como promover a conscientização e a educação sobre a violência doméstica digital. Nesse mundo cada vez mais conectado, é fundamental entender que a violência doméstica não se limita ao ambiente físico, mas também pode se estender ao espaço digital. As vítimas devem ter seus direitos protegidos, tanto no mundo real quanto no virtual, e o direito digital desempenha um papel importante nesse aspecto.

É necessário um esforço conjunto entre governos, legisladores, organizações de direitos humanos e sociedade em geral para combater efetivamente a violência doméstica digital. Somente por meio de ações coordenadas e legislação apropriada, podemos proporcionar um ambiente seguro e proteger as vítimas dessa forma insidiosa de abuso. Portanto, é fundamental continuar avançando na área do direito digital, adaptando-o às necessidades emergentes da sociedade, garantindo que as vítimas de violência doméstica digital recebam a proteção e o apoio necessários para reconstruir suas vidas e viverem livremente, tanto no mundo físico quanto no virtual.

REFERÊNCIAS

APLICATIVO. https://g1.globo.com/al/alagoas/noticia/2023/03/15/aplicativo-ajuda-no-combateaviolencia-contra-mulheres-em-alagoas-saiba-como-usar.ghtml Acesso em 15 de março de 2023.

CHAVES, Clara. O uso da tecnologia no combate à violência contra a mulher. Disponível em: https://blogs.iadb.org/brasil/pt-br/o-uso-da-tecnologia-no-combate-violencia-contra- mulher/ Acesso em 19 de abril de. 2023.

DEL CARMEN, Gabriela. A tecnologia pode ser uma forte aliada na conscientização, acolhimento e denúncia de casos de agressão física, moral e sexual, em: https://forbes.com.br/forbesesg/2023/05/04/-plataformas-que-oferecem-suporteavitimas-de- violencia-contraamulher/ Acesso em 04 de maio de 2023.

FUNDAÇÃO OSVALDO CRUZ. Violência contra as mulheres no contexto da Covid-19. Disponível em: https://portal.fiocruz.br/noticia/violencia-contra-mulheres-no-contexto-da-covid-19/ Acesso em 24 de maio de 2023.

LUDGERO, Paulo Ricardo. A violência doméstica no Direito Digital. Disponível em: https://www.jusbrasil.com.br/artigos/violencia-domestica-e-o-papel-do-direito-digital-protegendo-vitimas-em-um-mundo-conectado/1854367312 / Acesso em 18 de julho de 2023

MACEDO, Joe Frida: a tecnologia contra a violência doméstica. Disponível em: https://www.tecmundo.com.br/internet/228748-frida-tecnologia-violencia-domestica.htm Acesso em: 03 de junho de 2023.

Menina de 10 anos estuprada por tio conseguiu realizar o aborto; direito é garantido pela Constituição Disponível em: https://www.opovo.com.br/noticias/brasil/2023/07/10/menina-de- 10-anos-estuprada-por-tio-conseguiu-realizaroaborto–direitoegarantido-pela- constituição.html Acesso em 10 de junho de 2023.

PICCOLOTTO, Letícia. Tecnologia pode ser uma grande aliada no combate à violência contra meninas e mulheres, colunista. Disponível em: https://olhardigital.com.br/2023/07/11/colunistas/tecnologia-pode-ser-uma-grande-aliada-no- combateaviolencia-contra-meninasemulheres/ e https://www.encartnoticias.com/tecnologia-pode-ser-uma-grande-aliada-no-combateaviolencia-contra-meninasemulheres/ Acesso em 11 de julho de 2023.

Capítulo 12

Tecnologia e a Imagem de Professor em Sala de Aula

Ricardo Bezerra

Estamos em uma nova era, a da tecnologia, apesar de que há muito que faz parte do nosso cotidiano. Porém, com a chegada da Pandemia com a COVID-19 nossas vidas passaram a ter uma dependência tecnológica sem precedentes, com mudanças radicais em todos os setores, onde o avanço dela será para o novo caminhar da humanidade, a partir de agora, uma escala sem retrocesso e sem sabermos até onde iremos dominando-a. Somos agora realmente seres humanos dependentes da tecnologia e a inteligência artificial passa a ser não um simples avanço, como, também, uma ameaça quando seu uso amplo e irrestrito por mentes despreparadas e descontroladas chegam a usar o referido avanço para manipular imagens e constranger pessoas com uma falsa nudez. Se chegamos a esse ponto, os malefícios serão bem maiores do que os benefícios.

Sofremos uma revolução tecnológica e teremos que nos adequar ao seu aceleramento que ocorre a cada dia, pela qual tivemos que nos reinventar aos termos do isolamento social como opção de sobrevivência, deixando para traz todo nosso comportamento social para entramos na social-tecnologia e com isto foi possível lutar pelos nossos trabalhos, família e estabelecimento de uma nova convivência social que nos marcará e nos mudará sempre. Não seremos mais apenas a criação; seremos, também, a criação do temor à nova pandemia e por ela a eterna busca de uma tecnologia cada vez mais avançada que nos permita sobreviver na arca do isolamento social navegando pelo mundo globalizado sem beijar o solo pátrio. Seremos cada vez mais universais!

A tecnologia já proporcionava a realização de cursos virtuais, treinamentos e com a presença já constante de cursos EAD (Ensino a Distância) a educação vem sofrendo a cada dia mais a influência da revolução tecnológica. Porém, não renunciávamos aos cursos presenciais de primeiro, segundo e terceiro graus. Era

fantástico o convívio escolar! Era permitido gravar trechos de aulas, explicações, bases para uma pesquisa ou estudo complementar[1]. Rapidamente nos vimos longe do ambiente escolar e do calor humano dos colegas e professores para habitarmos uma lápide fria da tecnologia de mão ou de uma mesa estática.

Começaram a chegar gravações e filmagens[2] para suprir a forma de transmissão do saber. Quanta mudança! Aulas por plataforma. Filmagens com Professores e conteúdos não acessíveis para todos. A discriminação social e econômica se apresenta feroz diante de todos da comunidade acadêmica (pais, alunos e professores). Poucos são aqueles que possuem acesso à tecnologia (computador, celular e internet).

Todos que puderam tiveram que aderir **às** aulas remotas ou gravadas devido **à** suspensão das aulas presenciais[3]. Foram muitas as adaptações. Com esta adesão ocorreu uma implementação da evolução tecnológica e cada Instituição de Ensino buscou adequar às aulas às condições tecnológicas existentes.

Esta implementação ocasionou o surgimento de um novo olhar para a educação e as ferramentas tecnológicas, impondo para o corpo discente e docente uma nova postura e quebra de paradigmas. O empresariado educacional teve que investir em equipamentos e profissional de TI. Os professores tiveram que expor timidez e técnicas educacionais. Surge um novo universo e nele estão inseridos os alunos que irão se adequar para uma nova metodologia, descobrindo caminhos sem a presença do professor, e os pais que sem previsão contratual não conseguem entender o grau de investimento e pensam apenas em redução de mensalidades. Os conflitos começam a surgir nas relações contratuais.

Ao foco do artigo nos vinculamos ao aspecto da evolução tecnológica a necessidade imprescindível das gravações e filmagens de Professores em sala de aula. Apesar de que antes desta fase efetiva da tecnologia aconteciam algumas filmagens ou gravações para anotações e apontamos como tese para estudo, sem que isto ocasionasse grandes questionamentos. A contar deste marco regulatório pandêmico tudo mudou e, infelizmente, acredito que as empresas educacionais não contemplam em seus contratos, seja para com os pais ou alunos maiores de dezoito anos e nem mesmo com os professores as questões tecnológicas quanto **à** gravação e filmagem de aulas dos professores, nem quanto **às** condições de uso dessa nova ferramenta pelos pais e alunos. Fazemos aqui uma ressalva quanto a um tema específico e que não será abordado nesta matéria que é quanto ao uso da imagem dos alunos no ambiente escolar.

---

1 Lei 9.610/98 e seus incisos II e IV do art. 46

2 Aqui já podemos compreender como audiovisual pelo uso de imagem e som – letra i do inciso VIII do art. 5º da Lei 9.610/98

3 Decretos Estaduais e Municipais de Isolamento Social do primeiro semestre de 2020 – COVID-19

As Escolas e Universidades precisam primeiro adequar seus contratos para com os pais ou alunos que seja seus usuários e, também, como seu corpo docente quanto **às** revisões contratuais com acréscimo dos direitos envolvendo os dados pessoais[4], personalíssimos, de imagem[5] e de criação intelectual[6].

Os Contratos escolares precisam ter adequação com alunos, pais e professores para estabelecer os critérios, compatível a cada situação, do uso das gravações e filmagens das aulas[7]. O Contrato precisa estabelecer os limites de uso das ferramentas tecnológicas entre a instituição, alunos e professores. Precisa de uma temporalidade de uso e seu descarte[8].

Para os Alunos é necessário que alguns aspectos sejam privilegiados para que vede o uso sem limites e sem previsão contratual das gravações e filmagens que lhes são ofertados[9]. Criando responsabilidades para o aluno porque este material é de uso pessoal e intransferível, impedindo seu repasse ou reprodução total ou parcial, independente da forma e, principalmente, nas redes sociais ou grupos de WhatsApp. Aos alunos maiores de dezoito anos que respondem civil e penalmente podem ser, pelo descumprimento contratual, o polo passivo da uma reparação de danos materiais e morais[10] à exposição da imagem do Professor[11] com infringência ao regimento escolar e sua penalidade. Aos alunos menores de dezoito anos atribui-se a responsabilidade aos seus genitores ou responsáveis tutores de forma solidária que são os provedores pela educação dos filhos[12].

Para os Pais ou Alunos maiores de dezoito anos o contrato Escolar precisa de uma leitura sobre as novas regras tecnológicas e sua aplicabilidade educacional, propiciando um controle dos mesmos sobre o uso do material pelo filho menor de idade, já que serão os responsáveis pelos danos causados na reparação civil dos danos materiais e morais à instituição e ao Professor; podendo, ainda, incorrer em responsabilidade penal.

---

4 LGPD – Lei Geral de Proteção de Dados – Leis 13.709/2018 e alterações com a Lei 13.853/2019

5 CF, inciso X do art. 5º

6 Art. 13 da Lei 9.610/98

7 CF, Incisos XXVII e XXVIII do art. 5º

8 LGPD

9 Inciso VI do art 5º da Lei 9.610/98

10 CC – Art. 186 c/c 927

11 CC – Art. 20 – "Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais."

12 **"a execução de título extrajudicial por inadimplemento de mensalidades escolares de filhos do casal pode ser redirecionada ao outro consorte, *ainda que não esteja nominado nos instrumentos contratuais* que deram origem à dívida" -** STJ. 3ª Turma. REsp 1.472.316-SP, Rel. Min. Paulo de Tarso Sanseverino, julgado em 05/12/2017 (Info 618)

Ao Professor a relação contratual para com a Instituição alcança fronteiras além os muros da pessoa jurídica contratante, já que sua imagem e sua criação intelectual não são apenas uma ocorrência e presença física nas dependências da Instituição. O alcance ilimitado da transmissão do conhecimento precisa ser adequado aos contratos para que o Professor não exerça seu direito de vedação de uso por falta de previsão legal[13].

A nova relação contratual precisa estabelecer critérios da exploração econômica do contrato de trabalho que agora se empodera de uma materialidade da personalidade, dados pessoais, imagem e direito autoral moral[14] e da criação do intelecto[15] como direito autoral[16], sendo indispensável **à** autorização expressa[17] do Professor para uso externo da sua metodologia[18] diante dos novos equipamentos de uso para o exercício da profissão; pois, seus dados pessoais serão armazenados e expostos e precisam do seu trato de uso, com critérios de formação de dados e tempo de uso[19], não podendo deixar de enfocar a exposição de dados, de imagem, da intimidade e direito de personalidade.

A transmissão de conteúdo é algo que se tornou mais criterioso para análise contratual já que ser Professor requer uma carga genética na percepção popular de "está na veia" e que permite ao Professor o diferencial de se destacar dos demais, onde sua Técnica autoral de ministrar aulas é algo personalíssimo[20] e que se torna, em algumas vezes, uma "marca" e consequente "reserva de direitos" autorais pela criação do intelecto. Não podendo deixar de se abordar que ao Professor Universitário o amparo do STF ao "direito ao livre

---

13 CC – Art. 20 – citação 11

14 Art. 24 da Lei 9.610/98

15 "A doutrina do direito autoral qualifica como obra intelectual toda aquela criação intelectual que é resultante de uma criação do espírito humano (leia-se intelecto), revestindo-se de originalidade, inventividade e caráter único e plasmada sobre um suporte material qualquer. Como disse Henry Jessen: "A originalidade é condição sine qua non para o reconhecimento da obra como produto da inteligência criadora. Só a criação permite produzir com originalidade. Não importa o tamanho, a extensão, a duração da obra. Poderá ser, indiferentemente, grande ou pequena; suas dimensões no tempo ou no espaço serão de nenhuma importância. A originalidade, porém, será sempre essencial, pois é nela que se consubstancia o esforço criador do autor, fundamento da obra e razão da proteção. Sem esforço do criador não há originalidade, não há obra, e, por conseguinte, não há proteção". (Biblioteca Nacional - https://www.bn.gov.br/pergunta-resposta/que-obra-intelectual)

16 Inciso II do Art. 7º da Lei 9.610/98 – "as conferências, **alocuções**, sermões e outras obras da mesma natureza". (grifo nosso)

17 Art. 29 da Lei 9.610/98

18 **Buainain,** Antônio Márcio**:** "Possibilita transformar o conhecimento, em princípio um bem quase público, em bem privado e é o elo de ligação entre o conhecimento e o mercado."

19 LGPD

20 Os **direitos da personalidade** são normalmente definidos como o **direito** irrenunciável e intransmissível que todo indivíduo tem de controlar o uso de seu corpo, nome, imagem, aparência ou quaisquer outros aspectos constitutivos de sua identidade. (Origem: Wikipédia, a enciclopédia livre)

pensamento de ideias"[21] o torna na cátedra um diferencial de conhecimento e criação intelectual. Cabendo, portanto, reparação aos danos materiais e morais que venha a sofrer pela violação dos seus direitos constitucionais.

As aulas são, portanto, um repasse de conteúdo de uma atividade inerente ao Professor. Contudo, há de se compreender que a "criação do intelecto" é uma técnica autoral e que se reveste de direitos sobre sua habilidade e criatividade. Surge, portanto, o direito "moral" e a possibilidade de um direito autoral pela criação do intelecto, sem deixar de ser necessária a citação em qualquer caso como referência da fonte. A aula gravada ou filmada passa a ter o limite de reprodução parcial ou total conforme a previsão contratual[22].

Contudo, os reflexos pandêmicos são expressivos em toda a sua contextualização, visto que o mundo se curvou ao poder de uma pandemia e a humanidade passou, em todos os Continentes, por profundas alterações em suas relações familiares, sociais e trabalhistas. Porém, ressaltando que tudo isto compreende o aspecto tecnológico onde a instrução educacional cabível ao professor e a educação que deve ter sua origem familiar são, simplesmente, os eixos das grandes revoluções.

Em destaque o Brasil, nossa Pátria Continental, que na soma de milhares de vítimas e de famílias dizimadas, algumas em sua quase totalidade, teve por grandes momentos a visão de um deserto em suas avenidas e praças pela prisão domiciliar à qual fomos impostos a cumprir por determinação de uma legislação sanitária; onde, a revolução e evolução tecnológica nos fez, por obrigação de sobrevivência, avançar décadas na criação e uso do mundo digital. Ora, essa revolução teve por base a educação e nesta vertente a instrução pelos professores que entraram em nossos lares e se expuseram de todas as formas, buscando trazer conhecimento e que muitas vezes teve sua imagem arranhada, ofendida, denegrida por atos ilícitos de pessoas que ainda não aprenderam o que é "respeito", ou seja, *consideração, atenção, deferência, estima pelo que o outro é e pela sua existência*[23].

O que falar da pandemia no trabalho remoto e os aspectos do direito trabalhista?

O Jurista Cloves Manoel dos Santos afirma que *O home Office (aqui compreendido como todas as modalidades de trabalho remoto), foi uma saída mais segura de uma ação para atender aqueles serviços não essenciais.*

A revolução tecnológica flexibilizou as regras para o teletrabalho. Persegue-se, então, a preservação do emprego e a sustentabilidade do mercado. No caso específico do professor em sala de aula é preciso compreender que

---

21 CF, inciso IV do art. 5º

22 CF, inciso II do art. 5º

23 https://respeiteadiferenca.mpf.mp.br/www/respeite-diferencas.html

a preservação do seu emprego estava relacionado a vários fatores e não mais, apenas, ao seu conhecimento; seria, portanto, ter como requisito para manutenção do seu emprego o conhecimento e uso de tecnologia, elaboração de roteiro, ambiente adequado com equipamentos e iluminação, além de acústica e reservado, dicção, oratória, gesticulação, estética quando ao aspecto de produção pessoal, principalmente facial, e sem falar em vestuário, não podendo cair no descuido de ser filmado em trajes inadequados ou falar, quando ao vivo, coisas inoportunas que viessem comprometer a segurança do seu emprego. Então vejam que a imagem do professor passou a ter uma complexidade sem precedentes diante do universo que passou a atingir.

Diz Cloves Manoel dos Santos, ainda, que "*Ainda que seja impossível cravar o que é reservado aos modelos de legislação trabalhista, não dá para negar que a desburocratização e as novas tecnologias definirão outras regras para a relação no trabalho.*".

Surge assim, portanto, diz Cloves Manoel dos Santos que *o novo cenário de trabalho remoto deverá alcançar maior relevância nas considerações de alteração legislativa, tendo como fator de grande importância a saúde do trabalhador, físico e, principalmente, mental.*

Por fim, acrescente em tal previsão a criação de regulamentação mais assertiva e estruturada para o uso de tecnologias utilizadas na relação trabalhista, as quais terão prioridades aquelas que possuem versatilidade e adaptabilidade às inovações sociais na relação no trabalho.[24]

O pós-pandemia faz um divisor com seus reflexos onde já podemos de forma clara lembrar de um conceito histórico do uso de livros empoeirados e de folhas amareladas, com dobras em suas pontas e notas marginais; sem deixar de ter na memória as alergias que muitos apresentavam e que agora, alguns, não conseguem mais nem pegar em um livro de papel, dando-se como usuário exclusivo dos livros virtuais. São muitas as histórias que podemos agora inserir em nossos livros de memórias e da história educacional.

No pós-pandemia encontramos um novo mundo e novas descobertas nas relações pessoais, contratuais, judiciais e administrativo. São muitos os avanços que não admitem qualquer retrocesso. Digamos, inclusive, que é um passado que não volta. As escolas e universidades físicas existiram; contudo, a tendência é cada vez mais a ampliação de uma educação a distância.

Vivíamos em uma evolução tecnológica. Agora, passamos por uma gigantesca revolução tecnológica!

O trabalho não é mais um espaço físico. O trabalho está em todo lugar. Íamos de casa para o trabalho. Hoje estamos no trabalho.

A escola agora está nos apartamentos, casas, granjas, fazendas ou simplesmente de onde se encontre o Professor.

---

24 Santos, Cloves Manoel dos – Jusbrasil Newaletter

A Pandemia não atingiu classes. Todos foram aprisionados e atingidos por sua revolução tecnológica. Porém, no campo da educação o acesso da revolução tecnológica não é acessível a todos. Vivemos em um país continental de distorções econômicas e sociais sem precedentes, onde muitos não possuem, sequer, o que comer e imaginem um celular com internet e qualidade de sinal e onde o aparelho celular atenda as necessidades tecnológicas do aprendizado.

As *lives* não possuem na revolução tecnológica a figura do retrocesso. Digamos que não deixará de ser usada. Porém, o pós-pandemia no Direito Educacional impõe a volta do ato presencial do professor, seja como forma de manutenção da escola viva e/ou da sobrevivência da própria educação ministrada por profissionais capacitados para que não tenhamos a educação pelos próprios pais em substituição ao ensino tradicional.

Por analogia trazemos uma jurisprudência que pode melhor elucidar o quanto a tecnologia está vinculada ao Direito e, respectivamente, como a imagem do professor possui valor mercadológico e que precisa ser tratada, também, nos contratos profissionais:

> **DIREITO CIVIL. DANOS MORAIS PELO USO NÃO AUTORIZADO DA IMAGEM EM EVENTO SEM FINALIDADE LUCRATIVA.**
> O uso não autorizado da imagem de atleta em cartaz de propaganda de evento esportivo, ainda que sem finalidade lucrativa ou comercial, enseja reparação por danos morais, independentemente da comprovação de prejuízo. A obrigação da reparação pelo uso não autorizado de imagem decorre da própria utilização indevida do direito personalíssimo. Assim, a análise da existência de finalidade comercial ou econômica no uso é irrelevante. O dano, por sua vez, conforme a jurisprudência do STJ, apresenta-se in re ipsa, sendo desnecessária, portanto, a demonstração de prejuízo para a sua aferição. REsp 299.832-RJ, Rel. Min. Ricardo Villas Bôas Cueva, julgado em 21/2/2013.

O uso indevido de uma imagem poderá ocasionar danos materiais e morais e o professor usufruindo do princípio constitucional de que **"O direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem"** (inciso V, Art. 5º da CF), poderá requerer ressarcimento dos danos causados pelo infrator do ato ilícito, podendo, inclusive, também propor ação na esfera penal além da cível.

O Ato Ilícito ocasionado encontra amparo no Código Civil que em seu Art. 186, diz o seguinte:

> **"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".

O Dano moral não se prova, ele se presume na prova do ato ilícito e sua extensão irá promover a mensuração do referido dano, além da análise do reflexo econômico tanto de quem o causou como de quem foi a vítima, para que não haja o enriquecimento sem causa ou justificativa, ou seja, para que não haja fixação de valor sem a devida adequação ao caso e capacidade econômica das partes.

Entende-se que o dano moral está expresso no constrangimento sofrido pela parte/vítima que teve a sua imagem, honra e dignidade comprovadamente afetadas pelos atos do autor do ato ilícito, que usou da imagem do professor de forma indevida e/ou sem autorização, promovendo não só a dor física como, também, o constrangimento que será analisado diante das provas apresentadas para configuração do ato e sua extensão.

A configuração do dano moral se presume pelos fatos verídicos que foram narrados pelo professor que sofreu o dano, onde a tecnologia será hoje um grande instrumento ao seu favor porque em simples inspeção ou até mesmo em perícia irá identificar a caracterização do ato ilícito e o nexo de causalidade, promovendo a elucidação dos fatos e proporcionando amparo aos argumentos do professor. Portanto, ao serem usados instrumentos tecnológicos e o cometimento de ato ilícito é preciso entender o praticante do ato que poderá estar produzindo prova contra si mesma, visto que tudo realizado por equipamentos tecnológicos são rastreáveis. Isto serve de alerta para o uso da Inteligência Artificial ou do ChatGPT como ferramentas para causar danos ao professor no exercício da sua atividade ou até mesmo para atingir aspectos da vida íntima e dos seus dados pessoais.

> "A indenização por dano moral dispensa a prática de crime, sendo bastante a demonstração do ato ilícito praticado" (**STJ**-4ª Turma, Resp 163221-ES-DJU: 14.03.2000 – Rel. Min. Sálvio de Figueiredo Teixeira)
> "Dispensa-se a prova de prejuízo para demonstrar a ofensa ao moral humano, já que o dano moral, tido como lesão à personalidade, ao âmago e à honra da pessoa, por vezes é de difícil constatação, haja vista os reflexos atingirem parte muito própria do indivíduo – o seu interior. De qualquer forma, a indenização não surge somente nos casos de prejuízo, mas também pela violação de um direito". (**STJ-4ª T. Resp 85.019-RJ, Rel. Min. Sálvio de Figueiredo Teixeira).**

Sobre o assunto os doutrinadores, como se lê no Livro "Responsabilidade Civil e O Novo Código Civil" pág.45 e 46, do Desembargador Antônio Elias de Queiroga, aposentado do Tribunal de Justiça do Estado da Paraíba, diz:

> "Atente-se que o dano moral não reclama rigorosa demonstração probatória. È que, por atingir, fundamentalmente, bens incorpóreos, torna-se desnecessário

> que a vítima demonstre efetiva existência do dano. A prova do dano moral puro, portanto, cingir-se-á à existência do próprio ilícito, pois exigir-se que se provem situações íntimas (dor, aflição, angústia etc.) seria o mesmo que tornar irressarcido o dano moral."

O professor Yussef Sahid Cahali, monografista da matéria, assinala:

> " Tudo aquilo que molesta gravemente a alma humana, ferindo-lhe gravemente os valores fundamentais inerentes à sua personalidade ou reconhecidos pela sociedade em que está integrado, qualifica-se, em linha de princípio, como dano moral; não há como enumera-los exaustivamente, evidenciando-se na dor, na angústia, no sofrimento, na tristeza pela ausência de um ente querido falecido; no desprestígio, na desconsideração social, no descrédito à reputação, na humilhação pública, no devassamento da privacidade,(...) nas situação de constrangimento moral" e prossegue o citado mestre: Acentua-se cada vez mais na jurisprudência a condenação daqueles atos que molestam o conceito honrado da pessoa, colocando em dúvida a sua credibilidade e o seu crédito. Definem-se com tais aqueles atos que, de alguma forma, mostram-se hábeis para macular o prestígio moral da pessoa, sua imagem, sua honradez e dignidade."

Podemos concluir neste momento que a regra contratual estabelece uma formação e criação de dados que estão amparados na LGPD – Lei Geral de Proteção de Dados, impedindo seu compartilhamento, precisando de tratamento na forma do dispositivo legal para que não ocorra vazamento e venha ocasionar danos em sua violação. Precisa-se entender que quando colhemos dados estes precisam de tratamentos e quem tenha fornecido pode exigir as informações de como ocorre o tratamento e acesso aos mesmos. Portanto, o uso de dados pessoais de forma indevida, sem autorização expressa, irá com certeza proporcionar para muitos um grande transtorno e o que se vê no dia a dia é que as pessoas ainda não despertaram para isto e o dano que sofre sua imagem pelo uso indevido.

Uma gravação ou filmagem só encontra permissivo legal se for produzido como prova judicial ou administrativa[25], inclusive sem autorização judicial para casos de agressão, assédio, gênero, racismo etc.; alertando-se que, mesmo nestes casos, veda-se divulgação danosa.

O Professor é um criador de conteúdo e quando sua imagem é gravada ou fotografada e que na primeira situação, gravação, seu conteúdo é exposto também será alvo da ilicitude não só a imagem, mas ofensa aos direitos autorais do que esteja ali exposto como sendo um direito de propriedade privada que precisa de autorização para sua divulgação e do quantitativo de divulgação.

---

[25] Inciso VII do art. 46 da Lei 9.610/98

Encerrando, há uma nova ferramenta que parece inofensiva e que em determinados casos poderá ser de uso indevido se não for devidamente explicitado no contrato do Professor no exercício da sua função que é o podcast. Vejamos que o professor ao se permitir participar de um podcast para uma rede de ensino contribuirá para seu crescimento financeiro, digo, da empresa e não do professor, e que ficará em plataformas onde o seu saber não será remunerado. Portando, os meios tecnológicos utilizados para divulgação da empresa escolar por via da imagem do professor não precisa ser apenas o espaço físico da conhecida e antiga sala de aula; hoje, a sala de aula tem um conceito amplo de que é o espaço de onde o professor por meio de qualquer meio tecnológico ou presencial expõe seu conhecimento sobre área específica para ser transmitido ao público-alvo presencial ou virtual.

Capítulo 13
A Cultura do Like: A Cultura do Sharenting e a Responsabilidade Civil

Maynara Cida Melo Diniz

1. INTRODUÇÃO

Desde os avanços tecnológicos, crianças e adolescentes, são cada vez mais introduzidos neste meio e acabam não apenas por aprender as suas diversidades, como também se adaptam todos os dias para que haja não apenas sua inclusão no meio digital, como também no meio social.

Com isso, vem se tornando cada vez mais comuns, ver crianças e adolescentes de 0 até 17 com um celular, um tablet, kindle na mão, seja qual for a ferramenta, os menores, já sabem desde o nascimento manusear e utilizar em prol de si.

Porém, a grande preocupação começa com os menores de 0 á 12 anos, que apesar do conhecimento do que a ferramenta pode fazer, não tem uma exata noção que a mesma possa os expor a perigos inimagináveis, indo de comentários maldosos e até a utilização de suas imagens em sites de conteúdo adulto.

Tais mudanças sociais, não guiaram apenas a sociedade, como também os menores frutos desta relação e consequentemente, os genitores, que pela praticidade ao acesso da internet, acabam por colocar seu dia-a-dia para que todos tenham acesso, indeterminadamente se aquele que está sendo exposto, quer tal conduta ou não.

Com isso, se tornou cada vez mais comum, que os pais ou genitores postem seus cotidianos com seus filhos, mesmo que não seja da vontade dos menores aparecer nas redes sociais ou ainda, que estes não tenham noção daquilo que ocorre no meio digital com esta exposição exacerbada, acabam por ter suas privacidades colocadas no mundo digital.

Tal prática, tornou-se conhecida como "*sharenting*", que é classificado como a prática de exposição dos filhos em redes sociais, havendo ou não o seu

consentimento, o que poderia ou não acarretar danos ao menores, decorrentes dessa exposição no meio virtual.

Tal comportamento, apesar de ser cada vez mais comum, não deveria ser normalizado no meio social, tendo me vista justamente a privacidade de crianças e adolescentes e a sua possivel falta de noção daquilo que estão sendo submetidos.

Porém, tal exposição, cada vez mais característica vista em redes sociais de pessoas famosas, é uma prática, que até anônimos vem adotando e buscando uma vida glamourizada através da exposição infantil.

2. SHARENTING COMO PRÁTICA ABUSIVA

Conforme salientado, a prática de "sharenting", consiste no ato de que pais ou responsáveis compartilham nas redes sociais fotos, vídeos, ou quaisquer outras informações pessoais dos seus filhos, mesmo que seja apenas para mostrar o cotidiano destes, tal prática, além de ser normalizada, acarreta outras dificuldades e danos aos menores.

Assim, para Silvia Felipe (2019), classifica tal comportamento como:

> Entende-se como sharenting, portanto, a prática reiterada de compartilhamento, pelos pais ou responsáveis, de imagens e informações sobre a vida do filho e de seu cotidiano (escolas, atividades extras, viagens, etc) [...] O sharenting, por si só, possui aspectos jurídicos na própria relação entre a criança e quem posta a sua imagem ou suas informações. Fato é que, ainda que quem publique na rede tome alguns cuidados – como fazer posts apenas em ambientes privados – supondo que isso seja realmente possível na internet – a imagem da criança permanecerá na rede mundial de computadores por muitos anos, podendo causar a ela prejuízos ou embaraços em algum momento de sua vida (Felipe, 2019, online)

Diante da privacidade exposta e dos comportamentos decorrentes deste, o sharenting vem cada vez mais sendo debatido no meio social, justamente por haver em alguns casos, uma discordância por parte das crianças e adolescentes expostas, o que acarreta desde já uma não autorização para o uso de suas imagens.

É então que Eberlin (2017), faz a análise de que:

> A ideia de sharenting, também, abarca as situações em que os pais fazem a gestão da vida digital de seus filhos na internet, criando perfis em nome das crianças em redes sociais e postando, constantemente, informações sobre sua rotina. É o caso da mãe que, ainda grávida, cria uma conta em uma rede social para o bebê que irá nascer." (Eberlim, 2017, p.58).

Diariamente visualizamos as condições anteriores exemplificadas por Eberlin (2017), como o caso da digital influencer e empresária Vitória di

Felice Moraes, também conhecida no meio virtual como "Viih Tube", que ao descobrir sua primeira gestação, não apenas criou uma rede social para filha ainda durante a gravidez, como colocou cada passo da gravidez, o que fez da sua filha, não apenas uma mini influencer, como também, a menor, faturou o primeiro milhão de idade, antes do seu 1 (um) ano de idade.

Tal influencer, não foi a primeira a fazer a exposição de sua gravidez e com certeza não será a última, porém, nem sempre será apoiada, tendo em vista, que a privacidade da sua filha, foi atingida e sua hiperexposição não poderá ser mudada, pois o grande público que a acompanha requer sempre mais conteúdo da menor.

Tal conduta, chegou a originar um "cyberbullying" com a criança filha da influencer, desde quando esta nasceu, devido a sua fisionomia, seus jeitos, que mesmo sendo apenas um bebê, foi atacada por diversas vezes, vindo a influencer e o genitor a público, avisar que tomariam medidas judiciais contra aqueles que atacavam a pequena Lua Di Felice.

O cyberbullying é apenas uma das consequências trazidas pelo "sharenting", outros danos são causados devido a alta exposição do jovens, o que requer ainda mais cuidado com aquilo com os menores, pelo ordenamento pátrio.

Trata então, a lei Nº 8.069, DE 13 DE JULHO DE 1990, também conhecida como o Estatuto da Criança e do Adolescente-ECA, em seu art. 17:

> Art. 17. O direito ao respeito consiste na inviolabilidade da integridade física, psíquica e moral da criança e do adolescente, abrangendo a preservação da imagem, da identidade, da autonomia, dos valores, idéias e crenças, dos espaços e objetos pessoais.

Bem como trata o art. 18, do mesmo diploma legal:

> Art. 18. É dever de todos velar pela dignidade da criança e do adolescente, pondo-os a salvo de qualquer tratamento desumano, violento, aterrorizante, vexatório ou constrangedor.

Tal analise se torna primordial, não apenas para a proteção da criança e do adolescentes, como coibir a prática de "sharenting", praticada pelos genitores e/ou responsáveis.

3. O SHARENTING E SUAS CONSEQUÊNCIAS EM CRIANÇAS E ADOLESCENTES

Apesar do sharenting ser um comportamento comum visto na sociedade atual, tal prática poderá trazer consequências gravosas ao bem-estar de crianças e adolescentes, não somente o cyberbullying, como também doenças psicológicas.

Para a psicóloga Patrícia Bertozzi, "a exposição excessiva nas redes sociais pode causar inseguranças e problemas de autoestima e confiança entre os jovens", a mesma ainda explica, que durante a adolescência, comumente "os jovens enfrentam crises de identidade e baixa autoestima, características que os tornam vulneráveis na busca por conexões significativas e pertencimento", o que por si só já traria problemas psicológicos á este, em sua vida adulta.

Porém, quando os mesmos são expostos a rotinas mais pesadas e expostas em redes sociais, tais consequências podem se agravar e ainda piorar os transtornos que podem a ser desenvolvidos pelo indivíduo.

Para o psicólogo Anoberto Serafim, psicólogo de formação e coordenador geral da Casa da Criança e do Adolescente em Nova Friburgo, o mesmo afirma:

> "Os criminosos miram nas fragilidades e na vulnerabilidade. Há pessoas que se dizem bem intencionadas. Inicialmente, acolhem os jovens por meio de conversas e depois de ganharem a confiança, induzem-nos a enviarem fotos, vídeos íntimos, estimulam a prática de crimes ou mesmo sondam a rotina e dados de familiares para cometerem crimes." (SERAFIM, 2023)

A exposição dos menores, mesmo que seja para ser um "youtuber", um "streamer", influencer, ou apenas rotinas consideradas comuns, além das consequências mencionadas, ainda traz a baila, que estes ficam expostos á criminosos, que podem se utilizar de suas imagens, fotos, vídeos e informações pessoais, para sites adultos, ou ainda, para outros possíveis crimes.

De acordo com Streck (2019):

> Os pais têm o dever de proteger os filhos e isso inclui a proteção em relação à sua intimidade e privacidade. Quando os pais expõem os filhos na internet, seja por meio de postagens em redes sociais ou por outros meios digitais, podem estar violando a privacidade e intimidade dos jovens, o que pode acarretar responsabilização civil.

A necessidade de proteção vai além do alimento, moradia e o tratar bem o menor, mas toca-lhe igualmente a imagem, a dignidade e o dever de proteção deste, que conforme apontam Jameson e Webster (2019):

> "A exposição digital de crianças, impulsionada pelo compartilhamento de informações pessoais e imagens por parte de genitores nas redes sociais e outras plataformas, tornou-se uma parte intrínseca da cultura digital moderna" (Jameson; Webster, 2019, p. 235).

A conscientização deve acontecer primeiro nos pais, para que os filhos absorvam a proteção e os riscos que o meio virtual traz, devendo sempre ser

priorizado não apenas a consciência como o bem-estar e ainda, devendo ser claro que os riscos que estes podem se colocar, poderá ser irreversível, em detrimento a isso, Johnson (2020) trata:

> "Genitores têm a responsabilidade de compreender os riscos associados à exposição de seus filhos na internet e devem conversar abertamente com eles sobre como se proteger online. Isso inclui a importância de não compartilhar informações pessoais e de relatar qualquer comportamento inadequado na internet" (Johnson, 2020, p. 89).

O meio virtual, é um universo paralelo e muitas vezes, encantador para crianças e adolescentes, pois quando criados desde cedo no meio tecnológicos, tendem a ficar mais alienáveis com o passar da idade e a conexão, tende a se tornar um vício para estes.

Em alguns casos, a alta exposição a telas desde as primeiras idades, fazem com que algumas crianças fiquem agressivas, por justamente não haver o controle da exposição a internet, por parte dos pais.

Tal exposição exacerbada e sem o controle, podem fazer com que crianças e adolescentes tenham acesso a conteúdos agressivos, lesivos a vida ou ainda, a pornografia, o que irá atingir diretamente o desenvolvimento psíquico e motor deste.

4. A RESPONSABILIDADE CIVIL PELA PRÁTICA DE SHARENTING

Ao se entender o que o sharenting provoca e ainda, suas consequências, entendemos que há uma certa responsabilidade por parte daqueles que publicam e/ou compartilham conteúdos de sua vida privada que contenham crianças e adolescentes.

Classifica então Diniz (2015) como responsabilidade civil:

> A responsabilidade civil é a aplicação de medidas que obriguem uma pessoa a reparar dano moral ou patrimonial causados a terceiros, em razão de ato por ela mesma praticado, por pessoa por quem ela responde, por alguma coisa a ela pertencente ou de simples imposição legal. (Diniz, 2015, p. 35)

A responsabilidade civil é aquilo que deve ser reparado pelo dano causado, ou seja, todas as consequências abordadas anteriormente, devem ser reparadas, caso sejam cobradas.

Com isso, há ainda o pensamento de Gangliano e Pamplona Filho (2019):

> Responsabilidade civil é a imposição de um ônus, decorrente de ato lícito ou ilícito, que visa à reparação dos danos causados a outrem, por ação ou omissão

> do agente, lícita ou ilícita, ainda que por simples culpa." (Gagliano; Pamplona Filho, 2019, p. 41).

Assim como trata o art. 927 do CC/02:

> Art. 927. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.

Tais classificações e entendimentos pátrios no ordenamento juridico, são levadas em consideração, quando visualizadas que as consequências da hiperexposição infantil, trouxeram reflexos negativos na vida deste.

Que em alguns casos, podem desenvolver depressão, ansiedade e outras doenças psíquicas pela alta exposição, ou pior, pela cobrança de haver uma imagem límpida e controlada por parte dos menores, que nem sempre conseguirão segui-las.

Tal exposição, além de acarretar os prejuízos anteriormente abordados, pode ainda ensejar á indenização moral, á ser percebida por estes, tendo em vista, que estão tendo suas vidas "roubadas" ou ainda, "controladas" á ponto de não poderem se alto desenvolver.

Com isso, temos os dois tipos de responsabilidades, a "Responsabilidade Civil subjetiva e objetiva". "A responsabilidade civil subjetiva é a decorrente de dano causado em função de ato doloso ou culposo (negligência ou imprudência)". (Cavalieri filho, 2010, p. 16).

Para que haja a responsabilidade objetiva, não se faz necessário que se haja a culpa pelo ato praticado, que "Esta pode ou não existir, mas será sempre irrelevante para a configuração do dever de indenizar." (Gonçalves, 2012, p. 48).

Com isso então temos o pensamento de Gagliano e Pamplona Filho (2008, p.45):

> Responsabilidade, para o Direito, nada mais é, portanto, que uma obrigação derivada – um dever jurídico sucessivo – de assumir as consequências jurídicas de um fato, consequências essas que podem variar (reparação dos danos e/ou punição pessoal do agente lesionante) de acordo com os interesses lesados.

Com isso, nasce o dever de indenizar, reparar ou restituir o dano causado, não é um "mero dissabor", mas um enfrentamento que precisa de sua reconstituição, seja financeira ou moral, para que a vítima, tenha o mínimo de dignidade em sua existência.

Para Steinberg (2017), tal exposição poderia ser evitada caso os pais lessem afinco as diretrizes dos sites no qual expõe seus filhos:

> (...) os pais poderiam se familiarizar com as regras de privacidade dos sites em que hospedam fotografias de seus filhos, por eles compartilhadas; pais poderiam gerenciar as notificações desses sites para alertá-los quando as fotografias de seus filhos aparecem na pesquisa do google; pais deveriam considerar o compartilhamento anônimo ou de forma mais privada com pessoas específicas; pais deveriam evitar compartilhar fotos ou referencias com a localização de seus filhos para evitar identificação do domicílio ou escola deles; pais deveriam conceder a seus filhos o poder de 'veto' sobre o conteúdo a ser publicado em redes sociais, pais deveriam não compartilhar qualquer imagem ou registro de seus filhos sem roupas; e pais deveriam considerar em cada postagem feita o impacto delas no bem-estar atual e futuro de seus filhos, analisando o quão aquele conteúdo pode trazer consequências relacionais para eles. (STEINBERG, 2017, p. 879)

Lembra-se ainda, que o dever de reparar não é uma mera liberalidade, mas sim um dano decorrente de atitudes impensadas ou egoístas adotadas pelos pais ou genitores dos menores, que tentam a todo custo, uma busca pela aceitação social através das redes sociais.

5. CONCLUSÃO

Entende-se então que a conduta de exposição infantil adotada pelos pais e/ou responsáveis de crianças e adolescentes, além de ser uma postura lesiva ao emocional infantil, também agrega a uma reparação patrimonial que esse perfaria, caso sua vida viesse a ser atingida de forma ainda pior pela exposição imposta.

Deve-se ainda salientar, que tais consequências, quando constatadas, devem ser tratadas na raiz do problema e caso haja por vontade do agente lesado a vontade do cessar da sua imagem, esta deve ser respeitada, não apenas por estar incorrendo em crimes virtuais ou na própria Lei Geral de Proteção de Dados-LGPD, como também poderá está violando a liberdade, a expressão, o bem-estar e outros aspectos de crianças e adolescentes, conforme previsto na lei nº 8.069/90 e ainda, no atual Código Civil.

Neste sentido, a proteção do menor, não é apenas pela alta exposição da sua imagem a rede sociais, como também a exposição deste dentro do meio virtual, para que este não venha a ter acesso a conteúdo agressivos, lesivos ou ainda, a pornografia.

A proteção de crianças e adolescentes não deve ser apenas uma falácia ou uma mera expectativa, como também um dever de cada genitor para com os seus filhos, pois estes têm o direito de uma vida privada, sem uma hiper exposição por parte daqueles que deveriam lhe proteger.

Atualmente, o caminho adotado pelo ordenamento pátrio, encontra diversas barreiras imposta pelo próprio particular, que entende que a "vida é

sua" e poderá fazer o que quiser com ela, bem como daqueles que dependem de si.

Tal pensamento, apesar de absurdo, é uma filosofia adotada por parte da maioria dos genitores e/ou responsáveis, devendo se combatida e enfrentada para que outros jovens não venham a sofrer com seus dados divulgados, sua vida exposta e sua rotina devassada apenas em prol de alguns "likes".

REFERÊNCIAS

BARROS, Lucas. Apud. SERAFIM, Anoberto. Exposição de jovens nas redes sociais. 31 de maio de 2023. Disponível em: < https://avozdaserra.com.br/colunas/al-m-das- montanhas/exposicao-de-jovens-nas-redes-sociais> Acesso em 30 de mai. De 2024.

EBERLIN, Fernando Buscher von Teschenhausen. Sharenting, liberdade de expressão e privacidade de crianças no ambiente digital: o papel dos provedores de aplicação no cenário jurídico brasileiro. Revista Brasileira de Políticas Públicas. Volume 7, N° 3, 2017. Disponível em:<https://www.publicacoes.uniceub.br/RBPP/article/download/4821/xml> Acesso em: 30 de jun. 2024.

CAVALIERI FILHO, Sergio. Responsabilidade civil no novo Código Civil. Revista EMERJ, n. 24, p. 35.

DINIZ, Maria Helena. Curso de Direito Civil Brasileiro, 29ª ed., São Paulo: Saraiva, 2015. Volume VII.

FELIPE, Silvia. O Sharenting e os Filhos de Pais Separados. Juristas, 20 de maio de 2019. Disponível em: <https://juristas.com.br/2019/05/20/o-sharenting-e-os-filhos-de- pais-separados/\> Acesso em: 30 de jun.2024.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. Novo curso de direito civil: responsabilidade civil. São Paulo: Saraiva Educação, 2019.

JAMESON, S., WEBSTER, E. Children's digital exposure: An analysis of social media sharing by parents. Cyberpsychology, Behavior, and Social Networking, 2019.

JOHNSON, A. Parental responsibility in the digital age: A guide to protecting children in the online world. Digital Parenting Journal, 2020.

LEI nº 10.406, de 10 de janeiro de 2002. Código Civil Brasileiro. Brasília, DF. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em 30 de jun. de 2024.

RIBEIRO, Mariana; Sciancalepre, Pietra Taino. Exposição nas redes sociais: como isso pode afetar os jovens?. julho 5, 2023. Disponível em: < https://revistaesquinas.casperlibero.edu.br/cotidiano/a-exposicao-nas-redes-sociais-como-isso-pode-afetar-os-jovens/> Acesso 30 de jun. de 2024.

STEINBERG, Stacey. Sharenting: Children's Privacy in the Age of Social Media (March 8, 2016). 66 Emory L.J. 839 (2017); University of Florida Levin College of Law Research Paper No. 16-41. Disponível em: < https://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1796&context=facultypub.> Acesso em 30 de jun. de 2024.

Capítulo 14

A Imersão de Novas Tecnologias e a Proteção de Dados de Crianças e Adolescentes: A Aplicação do art.14 da LGPD

Fabiane Trindade Ozorio
Flávia Christiane de Alcântara Figueira

INTRODUÇÃO

Com a imersão de novas tecnologias as crianças e adolescentes se tornaram mais vulneráveis no ambiente virtual, deste modo o trabalho destaca as hipóteses de proteção legal objetivando resguardar os titulares de possíveis danos. Neste ínterim, restou evidente a necessidade da implementação da Lei Geral de Proteção de Dados, para garantir os direitos fundamentais destes sujeitos na internet. Outrossim, será apreciada a análise do Art.14 da LGPD, quanto a diferenciação no conceito de criança e adolescente, ainda ressaltando o seguinte problema, quais as consequências da ausência do conceito de crianças e adolescentes podem interferir no tratamento de seus dados pessoais. Na oportunidade, em relação à metodologia aplicada foi elaborada mediante pesquisas bibliográficas sobre proteção de dados. Assim, diante da vulnerabilidade dos titulares, torna-se necessário a devida regulamentação no processo de tratamento de dados para prevenir futuros danos.

1. LEGISLAÇÕES CONTRIBUTIVAS PARA A PROTEÇÃO DE DADOS DE CRIANÇAS E ADOLESCENTES

1.1. A NECESSIDADE DA APLIACAÇÃO NORMATIVA

É notório que o avanço dos meios tecnológicos acompanhado das inúmeras inovações digitais fomentou as novas gerações a interagirem dentro destes ambientes tornando os usuários mais suscetíveis a cibercrimes e golpes online.

Haja vista, que atualmente a maior parte dos utilizadores são crianças e adolescentes, na faixa etária entre 9 a 17 anos, segundo o site Legal Grounds Institut, esclareceu que por serem menos vigilantes em relação à troca de informações tornam-se desprotegidas, pois grande parte das plataformas não incentivam um estado de cautela.

Ainda levando em consideração o cenário de hiperdigitalização e datificação massiva de conteúdos pessoais, conforme Santos (2022, p.67), "o nível de impacto à privacidade e à intimidade, fez que inúmeros países ao redor do mundo cuidassem de elaborar legislações protetivas dos dados pessoais". Neste seguimento, foi instaurado a LGPD na legislação brasileira. Perante o exposto, diversos entendimentos foram formados para apreciar a proteção de dados de crianças e adolescentes onde direciona sua maior preocupação para à privacidade e à segurança.

1.2. ESTATUTO DA CRIANÇA E DO ADOLESCENTE

No âmbito do ordenamento jurídico brasileiro o Estatuto da Criança e do Adolescente é um dos principais instrumentos normativos responsáveis por resguardar à inviolabilidade de direitos dos sujeitos considerados incapazes. Em consonância, destacamos que o dispositivo legal também pode ser utilizado como fundamento para garantir a segurança dentro do ambiente virtual, por intermédio de seus princípios e valores.

Em conformidade, segundo as premissas dos arts. 1° e 3° do ECA (BRASIL, 1990), que enaltecem o princípio da proteção integral objetivando amparar as garantias e direitos das crianças e adolescentes no meio digital. Em que pese, ainda mencionamos o princípio da prioridade absoluta que enfatiza a condição de pessoa em desenvolvimento para demonstrar sua fragilidade, atribuindo aos sujeitos um caráter especial considerando sua fase de formação, estando presente no Art.227° da Constituição Federal (BRASIL,1988), bem como no Art.4° do ECA (BRASIL, 1990).

Por fim, destacasse o princípio do melhor interesse, o qual objetiva solucionar os conflitos por meio da interpretação mais favorável da lei, neste viés segundo a autora Amin (2010, p. 12), explica que o fundamento precisa valer-se em proveito da dignidade humana sob "a primazia das necessidades da criança e do adolescente como critério de interpretação da lei". Assim, considerando o exposto, é de supra importância a implementação dos princípios para garantir os direitos inerentes as crianças e adolescentes.

1.3. LEI GERAL DE PROTEÇÃO DE DADOS

Torna-se evidente que os problemas provenientes da imersão de novas tecnologias transmitiram ao sistema legislativo o questionamento se os métodos

utilizados atualmente são eficazes para garantir a devida proteção. Diante disso, foi integrado a LGPD, no seu Art.14 (BRASIL,2018), prevê que o tratamento de dados de crianças e adolescentes tem de ocorrer em seu melhor interesse, neste sentido conforme Mello (2023), o texto normativo deve ser interpretado visando em primeiro lugar os titulares.

Em conformidade, também foi incluída a PEC 17/2019 acrescentando na Constituição Federal os incisos XII-A ao art. 5º, e o inciso XXX ao art. 22 (BRASIL, 1988), que regulamenta a proteção de dados pessoais, ademais destaca-se por ser uma geração totalmente vinculada as novas tecnologias estão mais sujeitas aos problemas que podem suceder dela. Diante disso, conforme preceitua Laterça (2021, p.18), "a presença dessa população no ambiente on-line presume a existência de um arcabouço legal e jurídico que garanta a devida atenção".

Assim, após a promulgação da LGPD, transcorreu a criação da Autoridade Nacional de Proteção de Dados (ANPD), sendo responsável por fiscalizar, orientar e regulamentar o efetivo cumprimento legislativo.

Em relação ao tratamento de dados de crianças e adolescentes a autoridade manifestou-se mediante a divulgação do Enunciado N 1°, que objetiva destacar os parâmetros utilizados nas avaliações de tratamento de dados orientando quanto a importância da aplicação do princípio do melhor interesse para efetuar o correto controle das informações, salientando que o princípio deve prevalecer independentemente da situação apresentada, tendo o controlador a incumbência de realizar uma avaliação cautelosa preservando o direito dos sujeitos.

Em face do exposto, deve-se destacar os preceitos norteadores do direito para assegura as garantias constitucionais e proporcionar o pertinente tratamento de dados de crianças e adolescentes.

2. DIREITOS FUNDAMENTAIS DA CRIANÇA E DO ADOLESCENTE NO AMBIENTE VIRTUAL

As garantias constitucionais aplicam-se para proporcionar direito de personalidade para crianças e adolescentes que atribui todos os direitos relacionados a persona abrangendo, tanto seu corpo, quanto seu nome, imagem e toda característica que seja passível de identificar sua identidade. Ademais, os riscos trazidos pelo compartilhamento indevido de alguns dados da vida privada e íntima do titular expõe sua vulnerabilidade violando seu direito à liberdade de expressão e a sua privacidade, segundo Araújo (2021, p.13).

Na ocorrência, conforme Araújo (2021, p.13) as disposições constitucionais devem ser implementadas a fim de tutelar a proteção de crianças e adolescentes não se limitando apenas aos princípios legais da proteção integral e do melhor interesse.

Diante disso, o ambiente virtual deve promover segurança e proteção aos dados de criança e adolescentes respeitando os limites constitucionais sempre em favor de seus direitos. Portanto, sendo possuidor de toda tutelar legal não pode ter suas prerrogativas violadas pela inaplicabilidade da norma.

2.1. DEMONSTRAR A IMPRECISÃO DA LGPD QUANTO AO CONCEITO DE CRIANÇA E ADOLESCENTE EM SEU ART.14.

O ECA em seu art. 2°, distingue claramente "considera-se criança... a pessoa até doze anos de idade incompletos, e adolescente aquele entre doze a dezoito anos de idade" (BRASIL,1990), em contrataste o que não ocorreu na LGPD dificultando assim a interpretação e a aplicabilidade da norma.

No que concerne quanto a classificação do Art.14 da LGPD dirigisse de forma ampla dispondo todos em um mesmo rol, conforme demonstra o artigo "o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente" (BRASIL,2018), no entanto, sabemos que crianças e adolescentes devem possuir tratamentos distintos levando em consideração o seu grau de desenvolvimento.

Dessa forma, detemos o entendimento que o adolescente possui plena autonomia de expressar seu consentimento estando ou não na presença de seu responsável legal. Tal situação causa uma desproteção aos adolescentes que, tal como as crianças, ainda devemos considerar como pessoas em desenvolvimento, espelhando assim a sua vulnerabilidade

A vista disso, cabe ressaltar as demais formas de definição presentes no ordenamento jurídico, o Código Civil (BRASIL, 2002), realiza uma distinção divergente no que concerne a responsabilidade civil, evidenciando que os menores de 16 anos são considerados absolutamente incapazes e os adolescentes entre 16 e 18 anos são relativamente incapazes.

Em continuidade, referente ao adolescente a partir dos 16 anos, esses possuem capacidade relativa detendo aptidão de expressar sua vontade, nestes termos ante as hipóteses de tratamento de dados, o controlador delegado para realizar a coleta de informações deve solicitar o consentimento de forma direita ao adolescente, em consonância ao disposto no artigo 14 , § 6º da LGPD (BRASIL,2018),

Diante disso, presenciado tal transgressão, destinasse ao aplicador do direito ou utilizar a LPGD mesmo com a falta de definição dos sujeitos, ou adotar o ECA e suas interpretações doutrinárias, sendo que este não é o ordenamento especializado para o tratamento de dados pessoais de crianças e adolescentes.

2.2. O TRATAMENTO DE DADOS DE CRIANÇAS E ADOLESCENTES

Diante da análise do Art. 14° da LGPD, restou evidente que os aplicadores do direito encontraram dificuldades interpretativas no dispositivo legal, tornando-se assim complexa sua aplicação. Neste viés, os agentes devem tomar como referência os termos da LGPD, obtendo como base para o processamento as hipóteses dispostas no Art. 7°, que se destina aos requisitos para o tratamento de dados pessoais, bem como implementar os preceitos principiológicos enunciados no Art.6°.

Dentre as formas de controle de dados, se tratando de crianças e adolescentes o pressuposto legal utilizado deve ser o consentimento, o qual é procedido mediante a autorização específica do responsável legal, sempre com a transparência do tratamento aplicado e a finalidade das informações coletadas. Em consideração a premissa explicada, o consentimento se encontra regulado no Art.14, §1° da referida lei.

Considerando que o consentimento é utilizado como mecanismo para o procedimento de dados na hipótese de alguma violação, contudo cabe mensurar que com a falta de conceituação restou prejudicado o tratamento de dados direcionado para o adolescente. Pois, apenas advém a possibilidade para o tratamento de crianças, ficando o adolescente a mercê, não sabendo o legislador como efetuar e qual procedimento deve realizar, se solicita a autorização do consentimento para o próprio adolescente ou para o seu responsável legal.

No que pese a realização do exame de quaisquer bases legais aplicáveis ao tratamento de dados desses titulares, segundo Bioni (2020) terá como supra importância o balanceamento do melhor interesse, desde a verificação da validade ou até consentimento parental. Dessa forma, pelo fato de o melhor interesse ser um conceito de caráter eminentemente aberto, possuindo um parâmetro interpretativo, dependerá de precisas análises que confirmem se este interesse, de fato, foi alcançado.

2.3. RESPONSABILIDADE DOS AGENTES DE TRATAMENTO

Não obstante, quando nos referimos a crianças e adolescentes dentro do ciberespaço surge a preocupação quanto a sua segurança e privacidade. Destarte, é compreensível nortear que a responsabilidade de garantir a proteção a estes sujeitos recai perante todas as pessoas da sociedade, razão pela qual requer o chamamento das agências reguladoras para se comprometerem a respeito do devido tratamento dos dados das crianças e adolescentes.

Nesta situação, de acordo com a autora Mauk (2021, p. 6) a obrigação de controlar os conteúdos acessados e compartilhados pelos titulares vai além

da esfera parental, devendo também direcionar atenção para empresas prestadoras dos serviços. Nesse caso, os agentes de tratamento serão os indivíduos incumbidos para realizar a correta manipulação e processamento dos dados pessoais, ademais em casos de violação ou vazamento de informações poderão ser responsabilizados na seara civil com a reparação do dano causado.

Sendo assim, para evitar tais transgressões a coleta dos dados precisa ser executada por meio de "medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais" segundo o Art.46 da LGPD (BRASIL, 2018). Isto posto, merece destacar que os agentes de tratamento apenas responderam por seus atos praticados, tal como seus danos causados, sejam estes morais, materiais, individuais ou coletivos dentre as demais violações presentes no dispositivo legal.

3. IMPACTOS E OS DANOS CAUSADOS AS CRIANÇAS E ADOLESCENTES NO AMBIENTE VIRTUAL

Se por um lado, o ambiente digital é bastante positivo no que se refere à conteúdos educativos, de entretenimento e no sentido de efetivar o direito à informação, por outro lado pode ser palco de abusos de mercado de consumo, da pornografia infantil, da apologia ao crime e em alguns casos podem até gerar uma natureza mais grave como a incitação, a automutilação e o suicídio muitas vezes provenientes do cyberbullying.

Por esse motivo, com relação aos perigos presenciados na internet apontamos algumas ameaças, o qual estão expostos como a exploração sexual, a exposição de conteúdos inapropriados com caráter violento ou lascivos, ainda o compartilhamento e a produção artificial de materiais indevidos, bem como o sexting que é a autoprodução de imagens e vídeos sexuais realizadas pelas próprias crianças e adolescentes que estão sendo pressionados a enviar os arquivos para determinada pessoa que sem sua autorização divulga as informações.

Destarte, também mencionamos o cyberbullying que segundo Rodrigues e Alves, se caracteriza como uma intimidação, violência psicológica ou física que pode ser executada de maneira intencional e repetitiva, praticada de forma online por um indivíduo ou em grupo, para amedrontar, agredir ou adulterar dados pessoais objetivando criar constrangimento. Nesse caso, aludimos que um dos plausíveis meios de prevenir o ato poderia iniciar com o acompanhamento parental no ambiente virtual.

Outrossim, apontamos quanto ao abandono digital, em se tratando do encargo dos pais a autora Patrícia Peck Pinheiro, compreende o abandono digital como uma forma de negligência e omissão desencadeada pela desatenção parental em relação à segurança dos filhos no âmbito digital. Bem como, os autores Rodrigues e Alves destacam que "A falta de supervisão parental pode resultar em uma falta de percepção das consequências prejudiciais desse ambiente".

Em oportuno ressaltarmos o sharenting que consiste em outra prática ilícita desenvolvida na internet, caracterizada pelo excesso de divulgação de imagens de crianças e informações pessoais causando danos à privacidade e à segurança on- line. O escritor Gonçalves (2022, p.26) enfatiza que os riscos são ocasionados pelos próprios pais, mediante a superexposição de dados dos infantes compartilhadas nas redes sociais.

Diante o exposto, a proteção de dados de crianças e adolescentes no ambiente digital é um desafio constante, que abrange diversas áreas como o conhecimento jurídico, implementações de medidas técnicas, colaboração social e principalmente educação digital. A conjunção desses elementos e sua execução de forma efetiva pode contribuir para o desenvolvimento de um ambiente virtual mais seguro e protegido para as gerações futuras.

CONSIDERAÇÕES FINAIS

Destacou-se a vulnerabilidade das crianças e adolescentes dentro do ambiente virtual, enfatizando os riscos e os impactos causados ao seu desenvolvimento. Na sequência, frisamos sobre a principal problemática da pesquisa direcionada para a falta de definição de criança e adolescente no Art.14 da LGPD.

Outrossim, também foi conferida quanto as hipóteses de tratamento. Apesar da LGPD abordar quanto a proteção de dados pessoais da criança e do adolescente em seu artigo, muitas vezes essa responsabilidade ainda é direcionada para os responsáveis. No entanto, sabemos que a responsabilidade de preservar os diretos dos titulares são transmitidos a todos, devendo adotar o tríplice entre família, Estado e sociedade.

Na sequência ratificamos a importância da conscientização da sociedade quanto a instabilidade da segurança dos usuários na internet, tal como conferimos perante ANPD execuções e resoluções direcionadas ao problema apresentado. Ressaltamos que à segurança e à privacidade deve ser tratada com extrema urgência e prioridade, certificando que sempre seja exaltada a premissa básica a favor do melhor interesse diante da lacuna do Art.14 do texto normativo.

Diante o exposto, a LGPD reforçou os aspectos ligados à dignidade da pessoa humana, aplicando a doutrina da Proteção Integral e apresentando diretrizes específicas ao tratamento dos dados pessoais.

REFERÊNCIAS

AMIN, Andréa Rodrigues. **Princípios Orientadores do Direito da Criança e do Adolescente**. In: MACIEL, Kátia (Coord.). Curso de Direito da Criança e do Adolescente: Aspectos Teóricos e Práticos. 4. ed. rev. e atual. Rio de Janeiro: Editora Lumen Juris, 2010. p. 19-30.

ANPD (**Autoridade Nacional de Proteção de Dados**). Estudo preliminar hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes.2022. Disponível em:< https://www.gov.br/participamaisbrasil/enunciado-criancas-e- adolescentes.

ARAÚJO, Francisco Marcos de. **Concretização do direito fundamental à privacidade diante das novas tecnologias da informação**: **proteção de dados em ambiente virtual**. Fortaleza. Fundação Edson Queiroz Universidade de Fortaleza – centro de ciências jurídicas – programa de pós-graduação em direito constitucional – PPGD. 2021.

BIONI, Bruno; FAVARO, Iasmine; RIELLI, Mariana. **O tratamento de dados de crianças e adolescentes pode ser legal?.** Observatório Privacidade, 2020.

Disponível em: O tratamento de dados de crianças e adolescentes pode ser legal? – Observatório – Por Data Privacy (observatorioprivacidade.com.br).

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. 5 de outubro de 1988. Disponível em:< https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

BRASIL. Constituição (1988). **Proposta de Emenda à Constituição N° 17, DE 2019**. Proteção de dados Pessoais .Disponível em:< https://www25.senado.leg.br/web/atividade/

BRASIL. Lei nº 8.069, de 13 de julho de 1990. **Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências**. Disponível em:< https://www.planalto.gov.br/ccivil_03/leis/l8069.htm.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais**(LGPD). Disponívelem:<https://www.planalto.gov.br/ccivil_03/_ato20152018 /2018/lei/l13709htm.

Enunciado Cd/Anpd Nº 1, de 22 de Maio De 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-enunciado-sobre-o- tratamento-de-dados-pessoais-de-criancas-e-adolescentes/Enunciado1ANPD.pdf. Acesso em: 20/05/2024.

FICO, Bernardo. **Tratamento de dados pessoais de crianças e adolescentes**. Legal Grounds Institut. Disponível em: <https://legalgroundsinstitute.com/blog/tratamento-de-dados-pessoais-de- criancas-e-adolescentes/> Acesso em: 18/05/2024.

GONÇALVES, Thamires Oliveira. **Privacidade e proteção de dados pessoais da criança e adolescente**: uma análise acerca do direito de imagem e o direito a privacidade. São Paulo.2022.

LATERÇA, Priscilla Silva; FERNANDES, Elora; TEFFÉ, Chiara Spadaccini de; BRANCO, Sérgio (Coords.). **Privacidade e proteção de dados de crianças e adolescentes**. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; Obliq, 2021. E-book.

MAUK, M. **Parenting and the algorithm: a perspective on parental Controls and guilt amidst digital media**. In: Works in Progress • Algorithmic Rights and Pro- tections for Children, 2021, 1-9

MELLO, Pedro Santoro de. **Tratamento de dados de crianças e adolescentes**. São Paulo 2023.

PINHEIRO, Patrícia Peck. **Abandono digita**l. In: Direito Digital Aplicado 2.0., Coord. Patrícia Peck Pinheiro; São Paulo: Thompson Reuters/Revista dos Tribunais, 2ª. Edição, 2016

RODRIGUES, Murilo Almeida; ALVES, Rafael Rodrigues. **Desamparo na era digital: o impacto o mundo digital na vida de crianças e adolescentes sob uma perspectiva jurídica**. Disponível em: https://revistaft.com.br/desamparo-na-era- digital-o-impacto-do-mundo-digital-na-vida-de-criancas-e-adolescentes-sob-uma- perspectiva-juridica/. Acesso em: 20/05/2024.

SANTOS, Rômulo Marcel Souto dos, André Studart Leitão, and Erik Navarro Wolkart. **A responsabilidade civil na lei geral de proteção de dados pessoais e a regra de hand**. Revista Opinião Jurídica 20.34 (2022): 60. Print.

Capítulo 15

O Papel das Redes Sociais na Propagação de Crimes Cibernéticos

Camily Vitória Borges de Andrade Ribeiro
José Antônio de Oliveira Alves

INTRODUÇÃO

As redes sociais conectam indivíduos globalmente e facilitam a troca de informações, mas também propagam crimes cibernéticos. Este projeto explora o papel dessas plataformas na disseminação desses crimes, seus desafios e consequências. A pesquisa analisa como as redes sociais são usadas para crimes cibernéticos, como malware e roubo de identidade, e como essas plataformas se tornaram propícias para atividades criminosas. Justifica-se o projeto pela importância de entender essa relação. As redes sociais são alvos atraentes para criminosos devido à sua natureza aberta e facilidade de compartilhamento de informações, além da falta de regulamentação e anonimato que incentivam crimes.

A pesquisa qualitativa proporcionou uma compreensão dos fenômenos sociais e comportamentais relacionados aos crimes cibernéticos nas redes sociais, utilizando técnicas de coleta de dados como revisão bibliográfica, análise documental e estudo de casos.

1. CRIMES CIBERNÉTICOS

Os crimes cibernéticos ocorrem em ambiente virtual e incluem estelionato e fraude. Para analisá-los, é necessário identificar se são virtuais, determinar o bem jurídico atingido e aplicar o tipo penal correspondente. Fragoso (2013) afirma que a classificação dos crimes no Código Penal baseia-se no bem jurídico tutelado. Crimes virtuais incluem atos contra sistemas de informática, dados ou programas, e infrações contra patrimônio, liberdade individual e propriedade imaterial (Ivete, Senise e Ferreira, 2015).

Pinheiro (2019) aponta a dificuldade de determinar onde ocorreu a conduta ilícita na Internet, destacando a necessidade de adaptações normativas. As Leis nº 12.735 e 12.737 de 2012 foram criadas para regular a informática e tipificar condutas, mas não foram suficientes para coibir crimes cibernéticos, gerando discussões sobre o Marco Civil da Internet. Kolling (2015) destaca ameaças como vírus e programas maliciosos, incluindo keyloggers e backdoors. A maioria dos ataques cibernéticos explora erros humanos (Alexandria, 2019). É nesse sentido que especialistas forenses digitais coletam e analisam evidências digitais para resolver crimes (Silva e Costa, 2019), utilizando ferramentas como Encase Forensic Edition e FTK (Ayers, Brothers e Jansen, 2014). É crucial, portanto, proteger sistemas de internet para evitar manipulação intencional ou não de informações confidenciais e dispositivos (Soares, Lemos e Colcher, 2015).

2. PAPEL DAS REDES SOCIAIS NA SOCIEDADE MODERNA

2.1. CONEXÃO GLOBAL E COMUNICAÇÃO INSTANTÂNEA

As redes sociais transformaram a maneira como nos conectamos e comunicamos, desempenhando um papel significativo na sociedade moderna. No entanto, essa revolução digital trouxe desafios, especialmente em relação à segurança da informação e à propagação de crimes cibernéticos. Alecrim (2013) destaca que criminosos cibernéticos utilizam as redes sociais para disseminar malware e enganar usuários. Alexandria (2019) ressalta a importância de políticas eficazes de segurança da informação para proteger os usuários de ameaças cibernéticas, especialmente em ambientes de pesquisa científica. Andrighi (2012), por sua vez, trata dos desafios jurídicos enfrentados pelos provedores de serviços online em relação à responsabilidade por conteúdos ilícitos. Binicheski (2011), por fim, analisa os diferentes regimes de responsabilidade civil aplicáveis aos provedores de internet em várias jurisdições.

Essas fontes destacam a complexidade das questões relacionadas à segurança da informação e à responsabilidade dos provedores de serviços online em um mundo cada vez mais digitalizado, onde as redes sociais desempenham um papel central na vida cotidiana das pessoas. É essencial que governos, empresas e usuários trabalhem juntos para enfrentar esses desafios e garantir um ambiente online seguro e confiável para todos.

2.2. INFLUÊNCIA NA OPINIÃO PÚBLICA E POLÍTICA

As redes sociais têm uma influência crescente na opinião pública e na política, moldando percepções, disseminando informações e influenciando decisões

políticas. Ayers, Brothers e Jansen (2014) destacam o papel fundamental das redes sociais na disseminação de informações políticas e na formação da opinião pública, onde as plataformas permitem que os usuários compartilhem notícias, discutam questões políticas e expressem suas opiniões rapidamente. O alcance massivo de redes sociais como Facebook, Twitter e Instagram permite que informações se espalhem rapidamente.

As redes sociais ajudam na construção de identidades políticas e na formação de comunidades online, onde os usuários se agrupam com pessoas que compartilham suas opiniões. No entanto, essas plataformas também facilitam a disseminação de desinformação e notícias falsas, distorcendo a percepção da realidade e minando a confiança nas instituições políticas e na mídia tradicional. É essencial que os usuários desenvolvam habilidades críticas de pensamento para avaliar as informações online. As plataformas de mídia social devem combater a desinformação e proteger o debate público, implementando políticas robustas de moderação de conteúdo e promovendo a transparência.

2.3. PRIVACIDADE E SEGURANÇA ONLINE

Na era digital, a privacidade e a segurança online são preocupações cruciais, com as redes sociais desempenhando um papel central na vida cotidiana. Ghafarian e Seno (2015) afirmam que a privacidade online é uma preocupação crescente, pois os usuários compartilham mais informações pessoais em plataformas de mídia social. Redes sociais como Facebook e Instagram coletam uma quantidade significativa de informações dos usuários, desde dados básicos até comportamentos de navegação. Esses dados são usados para segmentar anúncios e personalizar experiências, mas também podem ser alvo de ataques cibernéticos.

Cots e Oliveira (2014) destacam que o Marco Civil da Internet no Brasil, Lei nº 12.965/2014, estabeleceu princípios para o uso da internet, incluindo disposições sobre privacidade e proteção de dados dos usuários, observando, todavia, que a forma de retirada de conteúdo da internet piorou, pois as plataformas passaram a ter responsabilidade para determinar a legalidade dos conteúdos postados.

O desafio de garantir a privacidade e segurança online, nesse sentido, requer uma abordagem multifacetada, envolvendo ações individuais, regulamentações governamentais e medidas de segurança por parte das empresas de tecnologia.

3. RELAÇÃO ENTRE REDES SOCIAIS E CRIMES CIBERNÉTICOS

A relação entre redes sociais e crimes cibernéticos é complexa, refletindo a interação entre tecnologia digital e atividade criminosa. As redes sociais

proporcionam um ambiente propício para disseminação de informações e interação entre usuários, mas também facilitam atividades criminosas. Emerson Alecrim (2013) destaca que redes sociais são frequentemente utilizadas para disseminar malware e golpes online. As redes sociais facilitam a engenharia social, técnica usada por criminosos para manipular pessoas e obter acesso a informações confidenciais. Binicheski (2011) observa que as redes sociais fornecem um vasto "pool" de potenciais vítimas. Ghafarian e Seno (2015) apontam que redes sociais podem ser usadas para espalhar notícias falsas. Além disso, redes sociais são usadas para coordenar atividades criminosas. Ayers, Brothers e Jansen (2014) mencionam que grupos criminosos podem usar plataformas de mídia social para trocar informações sobre técnicas de hacking. A relação entre redes sociais e crimes cibernéticos suscita debates no campo jurídico, especialmente quanto à responsabilidade dos provedores de serviços. Segundo Capez (2015), as redes sociais ampliam o campo de atuação para atividades criminosas, como cyberbullying. A responsabilidade civil dos provedores de serviços de internet é crucial. Leonardi (2015) e Damásio (2018) abordam que a legislação brasileira busca equilibrar liberdade de expressão e proteção contra danos decorrentes de conteúdos prejudiciais.

3.1. FACILITAÇÃO DA COMUNICAÇÃO E COORDENAÇÃO PARA ATIVIDADES ILÍCITAS

As redes sociais proporcionam um ambiente virtual onde indivíduos podem se conectar instantaneamente e interagir globalmente, mas também facilitam atividades ilícitas. Ayers, Brothers e Jansen (2014) observam que redes sociais são usadas para trocar informações sobre hacking, compartilhar ferramentas e recrutar novos membros para grupos criminosos. A comunicação instantânea e a vasta rede de contatos tornam essas plataformas propícias para colaboração criminosa. Alecrim (2013), acrescenta que as redes sociais oferecem uma plataforma conveniente para compartilhar informações e coordenar atividades de forma clandestina, permitindo ainda que criminosos expandam suas redes e recursos, recrutem cúmplices, encontrem fornecedores de serviços ilegais e compartilhem informações sobre alvos potenciais.

Essa facilitação da comunicação para atividades ilícitas apresenta desafios significativos para a aplicação da lei e a segurança cibernética. As autoridades precisam desenvolver estratégias eficazes para investigar e desmantelar grupos criminosos online, além de promover a conscientização dos usuários sobre os riscos associados ao uso das redes sociais para atividades ilícitas.

3.2. ENGENHARIA SOCIAL E PHISHING

A engenharia social e o phishing são estratégias comuns usadas por criminosos cibernéticos para explorar a confiança dos usuários de redes sociais, manipulando-os para revelar informações sensíveis como senhas e dados financeiros. Ghafarian e Seno (2015) observam que a engenharia social se baseia na manipulação psicológica para obter acesso a informações confidenciais. Redes sociais oferecem aos criminosos um vasto pool de vítimas, permitindo criar perfis falsos, enviar mensagens fraudulentas e enganar os usuários. O phishing envolve a criação de mensagens e páginas falsas que se passam por fontes legítimas, como bancos ou contatos pessoais. Binicheski (2011) destaca que ataques de phishing são frequentemente disseminados por links em redes sociais.

Para se proteger, os usuários devem adotar medidas de segurança cibernética, incluindo a verificação de remetentes e links suspeitos antes de clicar, a configuração de privacidade adequada para limitar informações visíveis publicamente, a educação contínua sobre ameaças e técnicas de ataque através de treinamentos sobre segurança cibernética, a adoção de autenticação de dois fatores (2FA) para adicionar segurança às contas online e a instalação e manutenção de software de segurança, como antivírus e firewalls. Implementando essas práticas, os usuários podem reduzir significativamente o risco de serem vítimas de engenharia social e phishing.

3.3. PROPAGAÇÃO DE MALWARE E GOLPES ONLINE

A propagação de malware e golpes online nas redes sociais é crescente e preocupante. Essas plataformas são terrenos férteis para atividades cibernéticas maliciosas devido à facilidade de acesso e ao vasto número de usuários. Alecrim (2013) explica que criminosos cibernéticos utilizam redes sociais para disseminar malware, explorando a confiança e a curiosidade dos usuários. Essas ameaças podem incluir links maliciosos, mensagens de phishing e aplicativos fraudulentos.

Malwares são programas projetados para causar danos ou roubar informações pessoais. Eles podem ser disseminados através de links aparentemente inofensivos em postagens ou mensagens privadas. Quando um usuário clica em um link infectado, o malware é instalado, permitindo que criminosos cibernéticos acessem informações confidenciais ou controlem o dispositivo remotamente. Alecrim (2013) destaca que criminosos aproveitam a natureza interativa das redes sociais para espalhar malware rapidamente.

Alexandria (2019) ressalta a importância de políticas de segurança da informação para proteger os usuários de ameaças cibernéticas. Em ambientes de pesquisa científica, a disseminação de malware pode ter consequências devastadoras, tornando essencial a implementação de medidas de segurança robustas.

Golpes online, como esquemas de pirâmide e fraudes de investimento, também são comuns nas redes sociais. Ghafarian e Seno (2015) observam que golpes online são frequentemente promovidos em redes sociais, visando enganar os usuários e obter lucro ilegal. Golpistas criam perfis falsos e páginas fraudulentas que parecem legítimas, atraindo vítimas desavisadas.

Andrighi (2012) discute os desafios legais enfrentados pelos provedores de serviços online em relação à responsabilidade por conteúdos ilícitos. Embora os provedores tenham a responsabilidade de monitorar e remover conteúdo malicioso, a vasta quantidade de informações compartilhadas torna essa tarefa difícil. Equilibrar a liberdade de expressão e a proteção dos usuários é um desafio contínuo.

Beal (2015) destaca que a educação dos usuários é fundamental para prevenir a disseminação de malware e golpes online. Ela sugere que organizações invistam em treinamentos sobre segurança cibernética para conscientizar os usuários sobre os riscos e as melhores práticas, incluindo a verificação de links suspeitos, a atualização de softwares de segurança e o uso de senhas fortes e únicas.

Criminosos cibernéticos utilizam técnicas de engenharia social para enganar os usuários e obter informações confidenciais. Peixoto (2016) observa que a engenharia social explora a confiança e ingenuidade das pessoas para obter acesso a dados sensíveis, como criando perfis falsos que se passam por amigos ou colegas de trabalho.

A propagação de malware e golpes online nas redes sociais apresenta um desafio significativo para a segurança cibernética. Empresas de tecnologia devem implementar políticas de segurança robustas e desenvolver ferramentas para detectar e remover conteúdo malicioso. Simultaneamente, os usuários devem ser educados sobre os riscos e as melhores práticas para se protegerem online. A colaboração entre governos, empresas e indivíduos é essencial para criar um ambiente digital seguro.

CONSIDERAÇÕES FINAIS

As redes sociais desempenham um papel significativo na propagação de crimes cibernéticos devido à sua natureza amplamente acessível e interativa.

Plataformas como Facebook, Twitter e Instagram permitem que criminosos cibernéticos alcancem um grande número de pessoas rapidamente e com relativa facilidade. Esses criminosos se aproveitam da confiança e da falta de conhecimento técnico de muitos usuários para realizar ataques como phishing, roubo de identidade e disseminação de malware.

A vasta quantidade de informações pessoais disponíveis facilita a personalização de ataques, tornando-os mais eficazes e difíceis de detectar. As redes sociais também proporcionam um ambiente propício para a criação e disseminação de

fake news e golpes financeiros, exacerbando os riscos para os usuários. A anonimidade oferecida por essas plataformas dificulta a identificação e a captura dos criminosos, tornando a aplicação da lei um desafio. Enquanto as redes sociais oferecem inúmeros benefícios em termos de comunicação e conexão, elas também apresentam um terreno fértil para atividades criminosas cibernéticas.

A conscientização do usuário, juntamente com medidas de segurança robustas e políticas de regulamentação eficazes, são essenciais para mitigar esses riscos e proteger os usuários contra ameaças cibernéticas.

REFERÊNCIAS

ALECRIM, Emerson. **Vírus de computador e outros malwares:** o que são e como agem. Infowester. 2013.

ALEXANDRIA, João C. S de. **Gestão de Segurança da Informação – Uma Proposta para Potencializar a Efetividade da Segurança da Informação em Ambiente de Pesquisa Científica.** São Paulo, 2019. 193f. Tese (Doutorado em Tecnologia Nuclear) - Universidade de São Paulo, São Paulo, 2019.

ANDRIGHI, Fátima Nancy. **A responsabilidade civil dos provedores de pesquisa via Internet.** n. 3. Rev. TST. vol. 78. São Paulo, 2012.

AYERS, R., BROTHERS S., & JANSEN, W. (2014, maio). ***Diretrizes sobre perícia de dispositivos móveis.***

BEAL, Adriana. **Segurança da informação:** princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2015.

BINICHESKI, Paulo Roberto. **Responsabilidade civil dos provedores de internet: direito comparado e perspectivas de regulação no direito brasileiro.** São Paulo: Juruá, 2011.

BRASIL. **LEI N°12.735**, de 30 de novembro de 2012. Brasília: Diário Oficial da União, 2012.

BRASIL. **LEI N°12.737,** de 30 de novembro de 2012. Brasília: Diário Oficial da União, 2012.

CAPEZ, Fernando. **Curso de processo penal.** 12.ed., São Paulo: Saraiva, 2015. ISBN 85-02-05002-8.

COTS, Márcio; OLIVEIRA, Ricardo. **Sistemática de retirada de conteúdo da internet piorou com o Marco Civil.** Consultor Jurídico, 10 set. 2014.

DAMÁSIO E. de J. **Direito Penal,** 29. ed. rev. atual. São Paulo: Saraiva, 2018.

DAHER, Aline Alves. **A responsabilidade civil dos provedores de hospedagem da Internet.** Escola da Magistratura do Estado do Rio de Janeiro, 2012.

DIMARIO, Giovana Alexandra; SOUZA, Luiz Felipe Camilo de. **Cyberbullying: estudo jurídico do fato. Cadernos de Iniciação Científica.** Faculdade de Direito de São Bernardo do Campo, ano 8, n 8. São Bernardo do Campo: FDSBC, 2011.

FARIAS, Robson Fernandes. **Introdução a química forense,** 2. edição, editora Átomo, p.14-15, 54,60- 2017.

GHAFARIAN, Ahmad; SENO, Amin Hosseini. **Análise da privacidade do modo de navegação privada por meio de Memória Forense**. Departamento de CSIS Faculdade de negócios de Mike Cottrell Universidade da Geórgia do Norte Dahlonega, GA 30005, EUA Syed. - No.16, dezembro de 2015

KOLLING, Gabriella S. **Segurança da informação.** 2015.

LEONARDI, Marcel. **Responsabilidade civil dos provedores de serviço de Internet.** São Paulo: Editora Juarez de Oliveira, 2015.

LONGHI, João Vitor Rozatti. **Marco civil da internet no brasil: breves considerações sobre seus fundamentos, princípios e análise crítica do regime de responsabilidade civil dos provedores.** In: MARTINS, Guilherme Magalhães (coord.). Direito privado e internet. São Paulo: Atlas, 2014.

MANDARINI, Marcos. **Segurança Corporativa Estratégica: Fundamentos.** Barueri: Manole, 2015, 344p.

MARCIANO, José L. P. **Segurança da Informação – uma abordagem social.** Brasília, 2016. 211f. Tese (Doutorado em Ciência da Informação) - Universidade de Brasília, Brasília, 2016.

MIRAGEM, Bruno Nubens Barbosa. **Direito Civil: responsabilidade civil.** São Paulo: Saraiva, 2015.

OLIVEIRA, Carlos Eduardo Elias de. **Aspectos Principais da Lei nº 12.965, de 2014, o Marco Civil da Internet: subsídios** à **comunidade jurídica.** Brasília: Núcleo de Estudos e Pesquisas/CONLEG/ Senado, abr./2014.

PAES, V. F. **Do inquérito ao processo: análise comparativa das relações entre polícia e ministério público no Brasil e na França.** Dilemas - Revista de estudos de conflito e controle social, v. 3, p. 111-141, jan./mar. 2015.

PEIXOTO, Mário C. P. **Engenharia Social e Segurança da Informação na Gestão Corporativa.** Rio de Janeiro: Brasport, 2016.

SANTOS, L. A. L. **O impacto da engenharia social na segurança da informação.** 2014. 82 f. Monografia (Especialização)- Universidade Tiradentes, Aracaju, 2014.

SILVA, M. H. L. F. da; COSTA, V. A. de S. F. **O fator humano como pilar da Segurança da Informação: uma proposta alternativa.** Serra Talhada (PE), 2019.

SOARES, Luiz Fernando Gomes; LEMOS, Guido; COLCHER, Sérgio**. Redes de computadores**: das LANs, MANs e WANs às redes ATM. 2. ed. Rio de Janeiro: Campus, 2015.

SHAFQAT, Narmeen. **Investigação forense da atividade da Web do usuário no Google Chrome usando várias ferramentas forenses.** Revista Internacional de Ciência da Computação e Segurança de Redes, VOL.16 No.9, setembro de 2016.

STOCO, Rui**. Tratado de responsabilidade civil: doutrina e jurisprudência.** São Paulo: Revista dos Tribunais, 2014.

TEFFÉ, Chiara Antonia Spadaccini de. **Responsabilidade civil e liberdade de expressão no Marco Civil da Internet: a responsabilidade civil dos provedores por danos decorrentes de conteúdo gerado por terceiros.** Revista de Direito Privado, vol.63, ano 16, p.59-83. São Paulo: Ed. RT, jul./set. 2015.

TEIXEIRA, Tarcisio. **Marco Civil da Internet: comentado.** São Paulo: Almedina, 2016.

Capítulo 16

Segurança Cibernética: Regulamentação e Medidas de Proteção Contra Ataques Cibernéticos

Thais de Souza Carrera
Flávia Christiane de Alcântara Figueira

1. INTRODUÇÃO

A segurança cibernética é um tema de crescente importância na era digital em que vivemos. Diversos fatores contribuem para a caracterização desta área, sendo alguns deles fundamentais para a compreensão e efetiva implementação de medidas de proteção. Em primeiro lugar, a confidencialidade dos dados é um pilar essencial da segurança cibernética. Proteger informações sensíveis de acessos não autorizados é crucial para preservar a privacidade dos indivíduos e a integridade de sistemas críticos.

Conforme Castells (2017), a revolução industrial fez com que a atuação do trabalhador sofresse uma mutação em sua rotina e em sua forma de organização familiar. Originalmente, o propósito da revolução tecnológica era fazer com que houvesse a otimização do tempo e com a atuação de máquinas, haveria a clara possibilidade de se obter a potencialização da produção, podendo de modo conjunto fazer com que o corpo proletariado obtivesse o potencial de administrar melhor o seu tempo e tivesse também a oportunidade de desfrutar da companhia de todos.

A revolução tecnológica objetiva ainda a otimização de tempo, a maximização na produção associada à qualidade de produção e também a melhoria nas condições de trabalho ao trabalhador. Contudo, tem-se observado certa dificuldade na adequação comportamental do trabalhador, uma vez que se tem tido – de modo consideravelmente relevante – reações controversas aos padrões do ambiente de trabalho referente ao mau uso de tecnologia na esfera laboral. (ÁVILA 2016)

Outro fator determinante é a integridade dos sistemas e redes. Garantir que os dados não sejam alterados ou corrompidos, seja por ações maliciosas ou

falhas acidentais, é primordial para a confiabilidade das operações e a tomada de decisões informadas. A disponibilidade também se configura como um elemento-chave da segurança cibernética. Assegurar que os recursos e serviços digitais estejam acessíveis aos usuários autorizados, mesmo diante de ameaças como ataques de negação de serviço, é indispensável para a manutenção do funcionamento normal das atividades.

A resiliência dos sistemas é um fator fundamental. A capacidade de recuperação e continuidade das operações após a ocorrência de incidentes, bem como a implementação de mecanismos de detecção e resposta a ameaças, são aspectos cruciais para a mitigação de riscos cibernéticos. De modo geral, a segurança cibernética envolve a interação de diversos fatores, tais como confidencialidade, integridade, disponibilidade e resiliência, que em conjunto visam garantir a proteção de informações, sistemas e infraestruturas críticas no ambiente digital.

A Lei 13.709/2018 "dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais". Tendo seu escopo bem definido, essa lei se refere também, à uma série de mudança que são necessárias dentro das empresas, como pressuposto à adequação organizacional, trazida pela instituição da LGPD no contexto administrativo. Dentro das possibilidades de mudança e de todas as necessidades de adequação, é possível citar a eminencia da capacitação do corpo de trabalhadores, bem como os gastos com treinamento de pessoal, somada à necessidade de adequação de todo o corpo da organização para a sua atuação em um novo modelo organizacional que precisa seguir formas de tratamento de dados, totalmente diferenciadas.

2. ASPECTOS GERAIS SOBRE ATAQUES CIBERNÉTICOS E A SEGURANÇA DE DADOS

Em um mundo cada vez mais digitalizado, a segurança cibernética tornou-se uma preocupação crucial para indivíduos, empresas e governos. Com a crescente dependência de sistemas e redes de computadores, a proteção contra ameaças maliciosas, como hackers, malware e ciberataques, é essencial para salvaguardar informações valiosas e manter a integridade de nossos sistemas (AVILA, 2016).

Neste contexto, a implementação de medidas eficazes de segurança cibernética desempenha um papel fundamental. Isso inclui a adoção de políticas e procedimentos rigorosos, a utilização de ferramentas de segurança avançadas, o treinamento constante de usuários e a manutenção atualizada de sistemas e aplicativos. Somente por meio de uma abordagem abrangente e proativa poderemos mitigar os riscos associados a invasões maliciosas e garantir a confidencialidade, integridade e disponibilidade de nossos dados e infraestrutura digital (FRAZÃO 2018).

Diante desse desafio, é imperativo que todos os envolvidos – desde indivíduos até organizações – assumam sua responsabilidade e adotem as melhores práticas de segurança cibernética. Somente dessa forma poderemos construir um ambiente digital mais seguro e resiliente, capaz de proteger-nos contra ameaças cada vez mais sofisticadas e garantir a confiança necessária para o desenvolvimento tecnológico e econômico da sociedade (BITTAR, 2014).

Assim, de acordo com o Leonardi (2022), a crescente dependência da sociedade moderna em relação às tecnologias digitais trouxe à tona a importância da segurança cibernética. Nesse contexto, o desenvolvimento de práticas legais adequadas é fundamental para garantir a proteção de indivíduos, empresas e instituições contra ameaças cibernéticas.

Primeiramente, Ávila (2016) explica que é essencial que haja uma legislação abrangente que defina claramente os direitos e responsabilidades de todas as partes envolvidas. Essa estrutura jurídica deve abordar questões como a coleta e o processamento de dados pessoais, a notificação de incidentes de segurança, a responsabilização por danos causados por ataques cibernéticos e a cooperação internacional na investigação e combate a crimes virtuais.

Além disso, as autoridades competentes devem estabelecer regulamentos e padrões técnicos que orientem as organizações sobre as medidas de segurança que devem ser implementadas. Esses requisitos normativos podem abranger desde a adoção de tecnologias de criptografia até a capacitação de profissionais especializados em segurança da informação (AVILA, 2016).

De acordo com o entendimento de Paesani (2016), é crucial que as práticas legais estejam em constante evolução, acompanhando as mudanças tecnológicas e as novas ameaças cibernéticas. Dessa forma, o arcabouço jurídico poderá se manter atualizado e eficaz na proteção dos cidadãos, empresas e instituições contra os riscos emergentes no ciberespaço.

Com isso, se avalia que, a construção de um ambiente seguro e confiável no mundo digital depende do desenvolvimento de práticas legais sólidas e atualizadas. Somente assim será possível garantir a salvaguarda dos direitos e interesses de todos os indivíduos e organizações que dependem das tecnologias de informação e comunicação.

2.1. MEDIDAS DE SEGURANÇA FÍSICA DE DADOS

A era digital trouxe uma abundância de oportunidades, mas também desafios significativos no que tange à responsabilidade pelo conteúdo online. À medida que a presença digital se expande, é imperativo que indivíduos, empresas e governos assumam uma postura proativa em relação à segurança cibernética (BITTAR, 2014).. Primeiramente, é fundamental compreender que a disseminação de informações online carrega consigo uma inerente responsabilidade.

Conteúdo impreciso, prejudicial ou até mesmo ilegal pode ter consequências devastadoras, afetando tanto indivíduos quanto a sociedade como um todo. Cabe a todos os atores envolvidos adotar medidas rigorosas de moderação e curadoria de conteúdo, a fim de mitigar os riscos (CASTELLS 2017).

Segundo o entendimento de Vanderlinde (2019), a segurança cibernética assume uma importância vital na era digital. Com o aumento exponencial de ataques cibernéticos, a proteção de dados pessoais, sistemas críticos e infraestruturas torna- se uma prioridade absoluta. Investimentos em tecnologias de segurança, programas de conscientização e políticas robustas são essenciais para salvaguardar indivíduos e organizações.

Segundo França, Faria, Rangel e Oliveira (2018), a responsabilidade pelo conteúdo online e a segurança cibernética são questões interdependentes que demandam atenção constante. Somente através de uma abordagem colaborativa e multifacetada, envolvendo todos os atores relevantes, será possível navegar com segurança neste novo paradigma digital, garantindo a proteção de todos os cidadãos. Ao observar o mercado consumidor atual, é fácil se deparar com diversas modificações observadas nas relações como um todo, especialmente as relações comerciais que ocorrem nas organizações privadas, neste âmbito, é válido dizer que são vários os caminhos percorridos pelos consumidores para adquirir produtos e serviços (FRAZÃO 2018).

As relações de negócio fazem parte da vida dos seres humanos em diversas localidades, utiliza-se desse recurso para que se troque produtos, serviços, informações e saberes, justamente pelo fato de que para o homem viver em comunidade é necessário assegurar uma variedade de recursos e mais que isso, é imprescindível a criação de vínculos como fator essencial para assegurar sua sobrevivência.

Nessa relação de trocas entre pessoas ou grupos, se criam vários mecanismos para que se possam estabelecer as maneiras de se comercializar e compartilhar absolutamente tudo (BRIDGMAN 2014).

Com a evolução da sociedade é pertinente que se tenha também uma evolução nas relações comerciais, neste caso, pode-se dizer que as mudanças irão afetar mais especificamente a divulgação de produtos e serviços aos consumidores, pois essa nova clientela traz consigo percepções do que se quer consumir de uma maneira diferenciada da existente no mercado consumidor. Essa nova visão requer uma proximidade por aquele que oferece o produto, além de características que sejam identificadas pelo consumidor como únicas e personalizadas (CALVO 2016).

Importante dizer ainda, segundo Cavalcanti e Santos (2018), que a neutralidade de rede é um princípio fundamental que garante a igualdade de tratamento do tráfego de internet, independentemente de sua origem, destino ou conteúdo. Nesse contexto, a sua relevância para a segurança cibernética é

inegável, uma vez que desempenha um papel crucial na proteção dos dados e informações que trafegam pela rede.

Assim, Vanderline (2019), ao assegurar a neutralidade de rede, evita-se a discriminação ou priorização de determinados tipos de tráfego, o que poderia ser aproveitado por atores maliciosos para contornar medidas de segurança ou realizar ataques direcionados. Isso garante que a rede seja um ambiente mais justo e seguro para todos os usuários, preservando a integridade e confidencialidade dos dados.

De acordo com o entendimento de Ebberrs e Van Dijk (2017), a neutralidade de rede possibilita a implementação efetiva de mecanismos de detecção e mitigação de ameaças cibernéticas, uma vez que não há restrições ou interferências indevidas no fluxo de informações. Isso permite que as soluções de segurança atuem de maneira mais eficaz, monitorando e respondendo prontamente a incidentes.

Horrigan (2019), explica que a neutralidade de rede é um pilar fundamental da segurança cibernética, garantindo a preservação da liberdade, privacidade e integridade dos dados que trafegam pela internet. Sua manutenção é essencial para a construção de um ambiente digital mais seguro e resiliente.

No panorama atual, encontra-se em Vanderline (2019), o fato de que a evolução tecnológica tem transformado profundamente as relações contratuais. Os contratos digitais e as assinaturas eletrônicas emergiram como soluções eficientes e convenientes, permitindo que indivíduos e organizações realizem negócios de forma ágil e remota. No entanto, essa transformação digital traz consigo a necessidade de abordar questões fundamentais relacionadas à segurança cibernética.

Junior (2019), cita que a adoção de contratos digitais e assinaturas eletrônicas envolve a transmissão e o armazenamento de informações sensíveis em ambientes virtuais. Portanto, é crucial implementar medidas robustas de segurança para garantir a integridade, confidencialidade e autenticidade desses acordos. Criptografia, autenticação de múltiplos fatores e armazenamento seguro de dados são alguns dos mecanismos essenciais para mitigar riscos de violação e fraude.

Para tanto, de acordo com Normandi (2019), ensinam que a conformidade legal e regulatória é um aspecto crucial a ser considerado. Leis e normas que regem a validade e a execução de contratos digitais e assinaturas eletrônicas devem ser rigorosamente observadas, a fim de resguardar os direitos e as obrigações das partes envolvidas.

Com isso, se percebe conforme se vê em Freitas e Pamplona (2018), que a adoção de contratos digitais e assinaturas eletrônicas traz consigo a necessidade de abordar questões fundamentais relacionadas à segurança cibernética. Ao implementar medidas de segurança eficazes e garantir a conformidade legal, é

possível aproveitar plenamente os benefícios dessa transformação digital, ao mesmo tempo em que se protege a integridade das relações contratuais.

A designação de que, com a LGPD, as instituições, terão a oportunidade de zelar ainda mais e proporcionar mais qualidade para seus clientes. Isso porque, em se tratando de organizações, há que se destacar o fato de que as informações de clientes, já recebem trato especial e já são protegidas em função do cuidado que se tem com a privacidade do cliente.

O cumprimento de todos os ditames presentes na LGPD, podem de início trazer contratempos à empresas de modo geral, isso porque toda a sua política de privacidade de dados terá que ser alterada e passará por ajustes com fins de adequação. No entanto, todo este processo trará resultados favoráveis para a empresa, uma vez, que, ao saber como lidar com os dados de seus clientes, a possibilidade de se fazer mal-uso destes é praticamente nula.

A implantação da LGPD é uma resposta à necessidade de normatização quanto ao tratamento dado ao grande número de informações aos quais se tem acesso nos dias de hoje. É comum a dúvida sobre como proceder com dados de clientes, uma vez que a tecnologia de fato encurtou distâncias e tornou a vida das pessoas de certa forma, transparente. Assim, ele crê ser pertinente os ditames dessa nova lei, que orienta sobre como proceder em relação aos dados dos clientes.

A percepção que se tem sobre o fluxo de dados de clientes ressalta a necessidade de normatização em relação ao trato que se deve ter com estes. Deste modo, o que se destaca aqui é o fato de que, mesmo no processo de gestão, há que se ter uma orientação quanto à conduta a ser adotada neste novo cenário que se descortina.

Em decorrência dessa nova necessidade, crê-se ser viável a implantação da LGPD, uma vez que as possíveis dúvidas que se pode ter sobre como proceder em tal situação, encontra-se abordada em sua definição e com acesso facilitado ao consumidor, proporcionado a este, a possibilidade de observar e de analisar cuidadosamente qual deverá ser a postura da organização em relação às informações à ela repassadas.

3. CONSIDERAÇÕES FINAIS

A segurança cibernética tornou-se uma preocupação fundamental na era digital atual. Com a crescente dependência de sistemas e plataformas online, é essencial que haja um arcabouço legal robusto para garantir a proteção dos cidadãos, empresas e instituições. Nesse contexto, os aspectos legais desempenham um papel crucial na promoção da segurança cibernética.

Um dos principais desafios é a constante evolução das ameaças cibernéticas, exigindo que a legislação acompanhe esse ritmo de mudança. As leis

devem abordar questões como a criminalização de atividades maliciosas, a responsabilização de provedores de serviços digitais e a definição de padrões de segurança mínimos. Além disso, a harmonização internacional das leis é fundamental para combater a natureza transfronteiriça dos crimes cibernéticos.

Outro aspecto relevante é a proteção de dados pessoais e a privacidade dos indivíduos. As leis de proteção de dados devem equilibrar a necessidade de segurança com o respeito aos direitos e liberdades fundamentais. Isso envolve regulamentações sobre coleta, armazenamento e uso de informações, bem como o estabelecimento de mecanismos eficazes de fiscalização e aplicação.

Adicionalmente, a promoção de uma cultura de cibersegurança depende da sensibilização e capacitação dos cidadãos. Nesse sentido, as políticas públicas devem contemplar ações de educação, treinamento e divulgação de boas práticas, empoderando a população para lidar com os desafios da era digital. Em suma, os aspectos legais referentes à promoção da segurança cibernética envolvem a constante atualização da legislação, a proteção de dados pessoais, a harmonização internacional e a disseminação de uma cultura de cibersegurança. Somente por meio de uma abordagem abrangente e efetiva, será possível assegurar a confiança e a segurança dos indivíduos, empresas e instituições no ambiente digital.

REFERÊNCIAS

ÁVILA, Humberto. Teoria **dos princípios: da definição** à **aplicação dos princípios jurídicos.** 6. ed. São Paulo: Malheiros, 2016.

BITTAR, Carlos Alberto. **Os direitos da personalidade.** 7. ed. Rio de Janeiro: Forense Universitária, 2014.

BRIDGMAN, Roger. Eletrônica. **Coleção Aventura na Ciência.** São Paulo: Editora Globo, 2014. Tradução: Anna Maria Quirino. Título original: Eletronics

CALVO, Adriana Carrera. **O uso indevido do correio eletrônico no ambiente de trabalho.** Jornal Trabalhista Consulex, Brasília, v. 20, n.959, mar. 2016, p. 6-13.

CASTELLS, Manuel. **A sociedade em rede.** Volume 1. 8 ed. São Paulo: Paz e Terra, 2017.

CAVALCANTI, Natália Peppi; SANTOS, Luiza Mendonça da Silva Belo. **A Lei Geral de Proteção de Dados do Brasil na era do Big Data.** In Tecnologia Jurídica & Direito Digital - II Congresso Internacional de Direito, Governo e Tecnologia. 2018.

DONEDA, Danilo. **Proteção de dados pessoais nas relações de consumo: para além da informação creditícia.** Brasília: SDE/DPDC. 2018.

EBBERS. W.E. VAN DIJK. J.A.G.M. **Resistance and support to electronic government, building a model of** innovation. Government Information Quarterly 24 (2017) 554–575

FRANÇA, T. C.; FARIA, F. F.; RANGEL, F. M.; FARIAS, C. M.; OLIVEIRA, J.. **Big Social Data: Princípios sobre coleta, tratamento e análise de dados sociais.** Artigo publicado nos anais do XXIX Simpósio Brasileiro de Banco de Dados (SBBD) 2018. Curi- Revista Jurídica da Escola Superior de Advocacia da OAB-PR Ano 4 - Número 1 - Maio de 2019 tiba. 2014, p. 8. Disponível em: http://www.inf.ufpr.br/ sbbdsbsc2014/sbbd/ proceedings/artigos/pdfs/127.pdf.

FRAZÃO, Ana. **Nova LGPD: principais repercussões para a atividade empresaria**l 2018. Disponível em www.jusbrasil.com.br

FREITAS, Cinthia Obladen de Almendra; PAMPLONA, Danielle Anne. **A complexa relação entre negócios e direitos humanos: as violações dos direitos de personalidade por meio de Tracking e Profiling em serviços online.** 2018 Disponível em www.jusbrasil.com.br

HORRIGAN. John B. **Americans Fall Along a Spectrum of Preparedness When it Comes to Using** Tech Tools to Pursue Learning Oline, And Manys Are Not Eager Or Ready To Take The Plunge. Pew Researche Center – Numbers, Facts and Trends Shaping the World. 2019

JUNIOR: Wagner Coppede. **Transformação Digital na Política Pública.** Fundação Getúlio Vargas - Escola De Administração De Empresas De São Paulo. S.P. 2019

LEONARDI, Marcel. **Tutela e privacidade na internet.** 1ª ed. São Paulo: Saraiva, 2022.

NORMANDI, Carolina. **Direito** à **intimidade do empregado X direito de propriedade e poder diretivo do empregador.** Síntese Jornal, Porto Alegre, v. 5, n. 56, out. 2019, p. 9-15.

PAESANI, Liliana Minardi. **Direito e internet.** 5ª ed. São Paulo: Editora Atlas S.A., 2016.

SOUZA, Marco Antonio Scheuer de. **O dano moral nas relações entre empregados e empregadores.** Erechim: Edelbra, 2023.

VANDERLINDE, Marcelo Ivo Melo. **Da Tecnologia:** Disponível em: <http://www.clubjus.com.br/?artigos&ver=2.25667&hl=no>.2019

VERGARA, Jerônimo Siqueira; DE ARAUJO, Luiz Ernani Bonesse; DA SILVA, Rosane Leal. **Direitos Emergentes na Sociedade Global**: Anuário do Programa de Pós-Graduação em Direito da UFSM. Ijuí: Editora Unijuí, 2019.

Capítulo 17
Plataforma do E-Notariado: Autorização Eletrônica de Doação de Órgão (AEDO)

Luisa Helena Cardoso Chaves

1. OS SERVIÇOS NOTARIAIS E DE REGISTRO

Primeiramente, importante analisar sobre a atividade notarial e registral. No atual ordenamento jurídico brasileiro, as atividades notariais e de registros são de organização técnica e administrativa destinados a garantir a publicidade, autenticidade, segurança e eficácia dos atos jurídicos. Os titulares das serventias notariais e de registros são profissionais do direito, dotados de fé pública, a quem é delegado o exercício da atividade notarial e de registro.

De acordo com o artigo 236 da Constituição Federal de 1988, os serviços notariais e de registro são exercidos em caráter privado, por delegação do Poder público:

> CF, Art. 236. Os serviços notariais e de registro são exercidos em caráter privado, por delegação do Poder Público.
> § 1º - Lei regulará as atividades, disciplinará a responsabilidade civil e criminal dos notários, dos oficiais de registro e de seus prepostos, e definirá a fiscalização de seus atos pelo Poder Judiciário.
> § 2º - Lei federal estabelecerá normas gerais para fixação de emolumentos relativos aos atos praticados pelos serviços notariais e de registro.
> § 3º - O ingresso na atividade notarial e de registro depende de concurso público de provas e títulos, não se permitindo que qualquer serventia fique vaga, sem abertura de concurso de provimento ou de remoção, por mais de seis meses.

Por muito tempo se discutiu sobre a natureza jurídica da atividade notarial e registral. Atualmente, é sabido que as atividades notariais e de registros possuem natureza pública, embora seu exercício seja particular, uma vez que

é um particular quem exerce tais funções. Tal entendimento foi devidamente sedimentado pelo seguinte julgado:

> EMENTA: AÇÃO DIRETA DE INCONSTITUCIONALIDADE. PROVIMENTO N. 055/2001 DO CORREGEDOR-GERAL DE JUSTIÇA DO ESTADO DE MINAS GERAIS. NOTÁRIOS E REGISTRADORES. REGIME JURÍDICO DOS SERVIDORES PÚBLICOS. INAPLICABILIDADE. EMENDA CONSTITUCIONAL N. 20/98. EXERCÍCIO DE ATIVIDADE EM CARÁTER PRIVADO POR DELEGAÇÃO DO PODER PÚBLICO. INAPLICABILIDADE DA APOSENTADORIA COMPULSÓRIA AOS SETENTA ANOS. INCONSTITUCIONALIDADE. 1. O artigo 40, § 1º, inciso II, da Constituição do Brasil, na redação que lhe foi conferida pela EC 20/98, está restrito aos cargos efetivos da União, dos Estados-membros, do Distrito Federal e dos Municípios — incluídas as autarquias e fundações. **2. Os serviços de registros públicos, cartorários e notariais são exercidos em caráter privado por delegação do Poder Público — serviço público não-privativo.** 3. Os notários e os registradores exercem atividade estatal, entretanto não são titulares de cargo público efetivo, tampouco ocupam cargo público. Não são servidores públicos, não lhes alcançando a compulsoriedade imposta pelo mencionado artigo 40 da CB/88 — aposentadoria compulsória aos setenta anos de idade. 4. Ação direta de inconstitucionalidade julgada procedente. (grifo nosso). ADI n. 2602 - Supremo Tribunal Federal.

Nesse sentido, de acordo com o julgado, o Supremo Tribunal Federal entendeu que os serviços registrais e notariais são exercidos em caráter privado por delegação do Poder Público, sendo considerados serviços públicos.

Corroborando o entendimento supramencionado, o autor Ceneviva[1] afirma que "no direito brasileiro, notário e registrador são agentes públicos, considerando-se que o Poder Público lhes delega funções, subordinados subsidiariamente, em certos casos, a regras colhidas no regime único previsto na Constituição, sem jamais atingirem, porém, a condição de servidores públicos".

Mas, afinal, quais são as finalidades das serventias extrajudiciais? Através do artigo 1º da Lei 8.935 de 1994 é possível entender quais as finalidades que a atividade busca e a grande importância dos atos extrajudiciais. Desta forma, consideram-se como fins de tais serviços: a publicidade, a autenticidade, a segurança e a eficácia dos atos extrajudiciais.

Portanto, a autenticidade consiste em declarar como verdadeiro o ato praticado pelo tabelião ou oficial de registro, uma vez que tais atos são dotados de fé pública. Ademais, os atos notariais e de registros têm finalidade de atribuir segurança aos usuários. Por sua vez, os atos são praticados com o fim de produzir efeitos jurídicos, ou seja, atingir a eficácia. E, por fim,

---

[1] CENEVIVA, Walter. **Lei dos Notários e Registradores Comentada (Lei n. 8.935/94)**, 4ª edição, ver. ampliada e atualizada, São Paulo/SP: editora Saraiva, 2002, p. 32.

a publicidade tem como intuito dar conhecimento geral quanto ao que foi praticado em determinada serventia.

Importante mencionar que no Brasil, as serventias extrajudiciais podem ter as seguintes atribuições: tabelionato de notas; tabelionato e registro de contratos marítimos; tabelionato de protesto de títulos; registro de imóveis; registro de títulos e documentos e civis das pessoas jurídicas; registro civis das pessoas naturais e de interdições e tutelas e registro de distribuição, conforme preceitua o artigo 5º da Lei nº 8.935/94 mais conhecida como Lei dos Notários e Registradores.

2. PLATAFORMA DO E-NOTARIADO: AUTORIZAÇÃO ELETRÔNICA DE DOAÇÃO DE ÓRGÃO (AEDO)

A atividade notarial existe há mais de 450 anos no país e considerando o avanço tecnológico, o serviço notarial e registral necessitou também se adequar às novas realidades tecnológicas. Antes da pandemia do Covid-19, houve a implementação no serviço notarial e registral de uma plataforma revolucionária chamada E-notariado que seria capaz de conectar às partes através de videoconferência para efetivar um ato notarial.

Neste momento, efetivou-se uma nova era: a implementação do sistema do e-notariado em todos os cartórios do Brasil. Vale destacar que o e-notariado é uma plataforma digital de serviços notariais desenvolvida pelo Colégio Notarial do Brasil – Conselho Federal (CNB/CF) juntamente com as seccionais de cada estado.

O provimento n. 100 de 2020 do Conselho Nacional de Justiça - CNJ permite que atos notariais sejam realizados através de videoconferência, assim como passou a permitir assinatura de documentos públicos através da referida plataforma (www.e- notariado.org.br).

O e-notariado garante eficiência e segurança aos atos notarias formalizados em meio digital. Portanto, diante da proibição de saídas às ruas através do Lockdown ou para aquelas pessoas acometidas pelo vírus que não podiam sair de casa, a plataforma passou a ser uma necessidade.

Conforme às necessidades foram surgindo, a plataforma do E-notariado foi evoluindo e ganhando novos atos eletrônicos. Recentemente, houve a implementação da Autorização Eletrônica de Doação de Órgãos – AEDO.

A Autorização Eletrônica de Doação de Órgãos - AEDO é uma forma eletrônica de autorizar a doação de órgãos, tecidos e partes do corpo humano. Importante destacar que a emissão da AEDO pelos cartórios é gratuita.

Realizada essa autorização, em caso de necessidade, o médico poderá acessar e agir de acordo com a declaração. O doador poderá autorizar a doação dos seguintes órgãos: coração, córneas, fígado, intestino, medula, músculo esquelético, pâncreas, pele, pulmão, rins e valva.

Para realizar a doação, necessário acessar o e-notariado usando seu certificado digital notarizado ou ICP-Brasil, preencher o formulário e selecionar um cartório para que providencie a AEDO com reconhecimento da assinatura por autenticidade. Após, o doador receberá por e-mail a referida declaração com a assinatura devidamente reconhecida por autenticidade.

Desta feita, quando necessário, os profissionais de saúde credenciados poderão verificar a existência e autenticidade de sua AEDO no sistema e providenciar os trâmites de doação dos órgãos autorizados. Caso o doador desejar acrescentar outros órgãos a uma AEDO já emitida, deverá revogar a anterior e fazer uma nova com todos os órgãos desejados, pois cada CPF somente poderá ter uma AEDO ativa. Nesse caso, contate o cartório emissor para maiores orientações.

Por todo o exposto, cada vez mais os serviços notariais e registrais estão sendo chamados para serem protagonistas de determinadas funções e com a Autorização Eletrônica de Doação de Órgãos – AEDO não foi diferente! Que a atividade notarial e registral do Brasil siga evoluindo tecnologicamente sempre!

REFERÊNCIAS

BRANDELLI, Leonardo. **Teoria Geral do Direito Notarial.** 2ª ed. São Paulo: Saraiva, 2007.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 25 jun. 2022.

BRASIL. Lei nº 6.015, de 31 de dezembro de 1973. **Dispõe sobre os registros públicos.** Casa Civil, Subchefia para Assuntos Jurídicos, 1973. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L6015compilada.htm. Acesso em: 25 jun. 2022.

BRASIL. Lei nº 8.935, de 18 de novembro de 1994. **Dispõe sobre os serviços notariais e de registros.** Casa Civil, Subchefia para Assuntos Jurídicos. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8935.htm. Acesso em 25 jun. 2022.

CENEVIVA, Walter. **Lei Dos Notários e Registradores Comentada.** São Paulo: Saraiva, 2000.

LOUREIRO, Luiz Guilherme. **Registros Públicos. Teoria e Prática.** 7. ed. Bahia: Juspodivm, 2016.

RIBEIRO, Luís Paulo Aliende. **Regulação da função pública notarial e de registro.** São Paulo: Saraiva, 2009.

RIBEIRO, Juliana de Oliveira Xavier. **Direito Notarial e Registral.** Rio de janeiro: Elsevier, 2008.