PROTEÇÃO

DE DADOS

COORDENAÇÃO:
PLINIO LACERDA MARTINS
SERGIO GUSTAVO PAUSEIRO

AUTORES:

Beatriz Bazaglia Sanches	Paula Cristiane Pinto Ramada
Bianca Paiva de Oliveira	Pedro Henrique de Paula Morais
Camila de Oliveira Lanor	Plinio Lacerda Martins
Carlos Alberto Pereira de Aguiar	Rafaela Gonçalves Duque
Isabella Macedo Torres	Roney Sandro Freire Corrêa
Luis Eduardo de Souza Leite Trancoso Daher	Sergio Gustavo Pauseiro
Marcella da Costa Moreira de Paiva	Simone de Oliveira Souza
Marcos Cesar de Souza Lima	Telson PiresWagner da Silva Reis

PUBLICAÇÃO: INSTITUTO DE DIREITO PUBLICO E PRIVADO - IDPP

Pesquisadores Organizadores da obra:
Marcella da Costa Moreira de Paiva
Paula Cristiane Pinto Ramada
Wagner da Silva Reis

APOIO: Universidade Federal Fluminense — PPGDIN

PROTEÇÃO DE DADOS

COORDENAÇÃO:

PLINIO LACERDA MARTINS

SERGIO GUSTAVO PAUSEIRO

Beatriz Bazaglia Sanches
Bianca Paiva de Oliveira
Camila de Oliveira Lanor
Carlos Alberto Pereira de Aguiar
Isabella Macedo Torres
Luis Eduardo de Souza Leite Trancoso Daher
Marcella da Costa Moreira de Paiva
Marcos Cesar de Souza Lima
Paula Cristiane Pinto Ramada
Pedro Henrique de Paula Morais
Plinio Lacerda Martins
Rafaela Gonçalves Duque
Roney Sandro Freire Corrêa
Sergio Gustavo Pauseiro
Simone de Oliveira Souza
Telson Pires
Wagner da Silva Reis

Pesquisadores Organizadores da obra:
Marcella da Costa Moreira de Paiva
Paula Cristiane Pinto Ramada
Wagner da Silva Reis

PUBLICAÇÃO: INSTITUTO DE DIREITO PUBLICO E PRIVADO - IDPP

2021

APRESENTAÇÃO

Estudos da Proteção de Dados Pessoais é um trabalho jurídico, fruto do resultado da pesquisa desenvolvida pelos pesquisadores do Grupo de Pesquisa de Proteção de Dados Pessoais do CNPQ, desenvolvido através de estudos desenvolvidos pelos alunos do curso de graduação e pós – graduação da Universidade Federal Fluminense – UFF e convidados, possuindo como líder o Professor Doutor Plinio Lacerda Martins e co-lider o Professor Doutor Sergio Gustavo Pauseiro durante o ano de 2020.

O Estudo envolve temas desde a questão das criptomoedas e os dados utilizados até as questões da inteligência artificial, realidade hoje cada vez mais presente na nossa sociedade informativa, envolvendo os dados pessoais do cidadão, apresentando problemas hodiernos enfrentados pelo usuário e as questões apontadas pela lei geral de proteção de dados pessoais e sua fiscalização e cumprimento, que é um desafio para a Agencia Nacional de Proteção de Dados.

Parabéns aos pesquisadores e aos doutorandos Marcella da Costa Moreira de Paiva, Paula Cristiane Pinto Ramada e Wagner da Silva Reis pela organização da presente obra jurídica, o nosso reconhecimento e homenagem.

MARTINS, Plinio Lacerda. PAUSEIRO, Sergio Gustavo. Estudos do Grupo de Proteção de Dados Pessoais – UFF. IDPP: Rio de Janeiro, 2021.

ISBN - 978-65-993766-2-7

LIVRO Digital.

SUMARIO

2

CIBERSEGURANÇA E RESPONSABILIDADE CIVIL DAS CÂMARAS ARBITRAIS POR VAZAMENTO DE DADOS PESSOAIS

Bianca Paiva de Oliveira
Marcella da Costa Moreira de Paiva
Sergio Gustavo Pauseiro

INTRODUÇÃO

A sociedade atual é norteada pelo paradigma tecnológico do processamento de informações, tornando a segurança da informação e a proteção de dados essenciais. Neste passo, este direito é colocado como o principal direito fundamental, diante da hiperconectividade. Contudo, deve vir em conjunto com medidas voltadas para a segurança da informação e a segurança cibernética. Cumpre ressaltar que tampouco os fabricantes de *internet of things* sabem dizer quais são as medidas necessárias para uma efetiva segurança de dados[1]. Tal incerteza e constante avanço tecnológico implica possíveis falhas de segurança, violações à proteção de dados pessoais e riscos para as instituições, bem como indefinições quanto à responsabilidade por vazamento de por culpa de terceiros.

A arbitragem e seus participantes não estão imunes aos novos paradigmas e suas demandas, ou seja, devem atentar à proteção de dados pessoais e à segurança da informação. Neste passo, propõe-se a análise da cibersegurança na arbitragem e a responsabilidade civil das câmaras arbitrais por vazamento de dados pessoais dos envolvidos, à luz da Lei Geral de Proteção de Dados e das *soft laws* relativas ao tema. O exame do mencionado objeto se dá a partir do método dedutivo e a pesquisa se baseia em revisão bibliográfica.

1. PROTEÇÃO DE DADOS E RESPONSABILIDADE CIVIL

É inegável que estamos em uma sociedade da informação, em que a tecnologia da informação e da comunicação aparece como o paradigma tecnológico como fonte de produtividade[2]. Este aspecto gera uma excessiva transparência das informações privadas das pessoas físicas e jurídicas, que dependem de colocar-se seus dados em risco para realizar negócios jurídicos e, inclusive, se relacionar na sociedade atual[3].

---

[1] MAGRANI, Eduardo**. A internet das coisas**. Rio de Janeiro: FGV Editora, 2018, p. 92.
[2] CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz e Terra, 1999, p. 54.
[3] HAN, Byung-Chul. **Sociedade da transparência**. Petrópolis, RJ: Vozes, 2017.

Sobre os marcos que originaram essa evolução, antes mesmo da criação da Internet, a informação já vinha figurando em um papel de centralidade. Para otimizar o desenvolvimento econômico a desmaterialização da informação, por meio dos *bits*[4], foi proporcionando a sua circulação de forma virtual, permitindo sua circulação de forma virtual, implicando em um crescimento exponencial na *quantidade* de informações processadas.

Assim, figura com papel de destaque a linguagem binária, por meio da qual permitiu-se o acúmulo de informação e a adoção de novas plataformas. Outro progresso possibilitado com essa linguagem, foi na ordem qualitativa no processamento dessa informação, sendo mais precisamente organizada, facilitando, em última análise, o seu próprio acesso. Em outras palavras, foi a conjunção destes dois fatores aliados e complementados pela criação da Internet, que virtualizaram a informação[5].

A *posteriori*, com a sedimentação da internet, o processo de evolução segue constante, aliado à introdução de tecnologias disruptivas nas mais variadas áreas, e consequentemente, sendo apresentados novos desafios. Eduardo Magrani, apresenta que o cenário de hiperconectividade envolve a relação entre objetos inteligentes, big data e inteligência da computação, que são conhecidas pela sigla - *analytics + big data + cloud computing*, e ausência de conhecimento sobre seus riscos e benefícios [6].

Na economia da informação, os dados pessoais dos cidadãos converteram-se em um elemento basilar. Onde, com a possibilidade de organizá-los de maneira mais escalável, como através do Big Data, criou-se um mercado cuja base de sustentação é a sua extração e comodificação, especialmente na área de marketing e publicidade[7].

É evidente que o direito à privacidade constitui um limite natural ao direito à informação[8]. No ordenamento jurídico brasileiro, a Constituição Federal de 1988 prevê em seu art. 5.º, 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. Stefano Rodotà, defende que a proteção é o direito fundamental mais relevante da atualidade, interferindo diretamente na democracia[9].

---

[4] *Bit* é a sigla para *Binary Digit*, que em português significa dígito binário, sendo a a menor unidade de informação que pode ser armazenada ou transmitida.
[5] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 8.
[6] MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV Editora, 2018, p. 25.
[7] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 12.
[8] PINHEIRO, Patricia Peck. **Direito digital**. 5. ed. rev.atual. e ampl. de acordo com as Leis n. 12.735 e 12.737 de 2012.São Paulo: Saraiva, 2013, p. 35.
[9] RODOTÀ, Stefano. **A vida na sociedade de vigilância**: a privacidade hoje. Rio de Janeiro: Renovar. 2008, p. 21.

Nesse cenário, é nítida a preocupação no que diz respeito a proteção desse direito da personalidade, inerente ao próprio homem e visa primordialmente resguardar a dignidade da pessoa humana. Assim, no ano de 2018 foi promulgada a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018. Se faz importante evidenciar há menções ao tratamento de dados em outros dispositivos legais nacionais, como no Código de Defesa do Consumidor, o Marco Civil da Internet (Lei 12.965/2014) e a Lei do Cadastro Positivo (Lei 12.414/2011), havendo um agrupamento dessas regras na LGPD, que representa um marco no empoderamento do titular, assim como, proporciona maior possibilidade de conformidade e fiscalização do cumprimento de seus preceitos.

No que concerne aos seus fundamentos, é colocado como objetivo do tratamento de dados pessoais, a proteção de direitos fundamentais como a liberdade, a privacidade e o livre desenvolvimento da personalidade humana. No art. 6° da referida lei, é previsto que essa atividade deverá observar a boa-fé princípios como o da transparência que consiste na garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial, tal como o da prevenção, com a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Além desses também podem ser citados a título de exemplo o da segurança, na qual devem ser utilizadas medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, assim como o da responsabilização e prestação de contas, por meio do qual deve haver a demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção e, inclusive, da eficácia dessas medidas.

No âmbito jurídico, as bases legais para tratamento de dados pessoais mais comuns são relacionadas à exceção de consentimento para cumprimento de contratos em geral, cumprimento de obrigações legais e para o exercício regular de direitos em processo judicial, administrativo ou arbitral. Entretanto, por se referirem a exceção apenas no que diz respeito ao consentimento do titular, não exime as agentes de tratamento de eventuais responsabilidades nas hipóteses de violação dos dados pessoais.

A Seção III da do Capítulo VI da LGPD trata acerca da Responsabilidade e do Ressarcimento de Danosnesse cenário[10]. Assim, o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação em comento, é obrigado a repará-lo, art. 42.

Walter Capanema defende que o uso da expressão "legislação de proteção de dados", demonstra o reconhecimento por parte do legislador da existência de um microssistema, com normas previstas em diversas leis, inclusas, desse modo as normas administrativas regulamentares que serão expedidas pela Autoridade Nacional de Proteção de Dados ou por outras entidades que versem sobre o tema[11].

Outro artigo de suma importância, é art. 46, por meio do qual é estabelecido que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Em consonância, é previsto no parágrafo único do art. 44, que responderá pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas.

Assim, no que diz respeito às hipóteses de responsabilidade prevista nesse diploma legal, podem ser classificadas como violação de normas jurídicas, do microssistema de proteção de dados ou pela violação de normas técnicas, voltadas à segurança e proteção[12], ondeé necessária a análise da mesma ter originado um dano moral ou material a um titular, ou até mesmo, a uma coletividade, sendo a extensão do dano levada em consideração na definição do *quantum* indenizatório.

Há ainda a previsão das hipóteses de exclusão da responsabilidade, previstas no art. 43 da LGPD. Nele é disposto que os agentes de tratamento só não serão responsabilizados quando provarem que não realizaram o tratamento de dados pessoais que lhes é atribuído, que, embora o tenham realizado , não houve violação à legislação de proteção de dados ou, por fim, que o dano é decorrente de culpa exclusiva do titular ou de terceiros.

---

[10] Violação de dados pessoais é uma violação da segurança que conduz à destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso a dados pessoais transmitidos, armazenados ou tratados de outro modo. Fonte: Regulamento Geral de Proteção de Dados (UE) 2016/679; Artigo 15(1).

[11] CAPANEMA, Walter Aranha**. A responsabilidade civil da Lei Geral de Proteção de Dados**. Cadernos Jurídicos da Escola Paulista da Magistratura, ano 21, nº 53. São Paulo. 2020, P. 165. Disponível em: <http://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_6_a_responsabilidade_civil.pdf?d=63725034755900571 2>. Acesso em: 27 set. 2020.

[12] CAPANEMA, Walter Aranha. **A responsabilidade civil da Lei Geral de Proteção de Dados**. Cadernos Jurídicos da Escola Paulista da Magistratura, ano 21, nº 53. São Paulo. 2020, P. 165. Disponível em: <http://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_6_a_responsabilidade_civil.pdf?d=63725034755900571 2>. Acesso em: 27 set. 2020.

Sendo assim, dado esse panorama, se mostra como essencial a formação de uma cultura pautada na conformidade com a LGPD, com um programa de *compliance* alinhado e uma governança de dados solidificada. Além disso, a preocupação com a segurança se apresenta como basilar, em uma sociedade que tem o valor dos dados ocupando uma posição de destaque.

2. CIBERSEGURANÇA NAS CÂMARAS ARBITRAIS

2.1. FUNÇÃO DE GUARDA DAS INSTITUIÇÕES DE ARBITRAGEM

Frente à proteção de dados pessoais regulamentada nas diversas jurisdições, as câmaras arbitrais necessitaram incorporar sistemas de segurança, seja no funcionamento administrativo da instituição ou nos procedimentos arbitrais. Estes envolvem dados privados de pessoas físicas e jurídicas, incluindo segredo industrial, e devem respeitar a salvaguarda destes. Ademais, a confidencialidade consiste em um dos princípios básicos da arbitragem e a proteção de dados entra como um dos seus aspectos coligados. Nesta direção, deve-se analisar a função das câmaras arbitrais e suas implicações na administração do procedimento e na guarda de dados pessoais, ao passo que se centra aqui na análise das instituições de arbitragem.

Primeiramente, cumpre destacar que a modalidade de arbitragem que se estuda, no presente artigo, é a institucional. Isto é, foca-se na abordagem da arbitragem em que as partes escolhem uma câmara arbitral para realizar a gestão do procedimento, que será em conformidade com o regulamento arbitral da instituição[13]. Com isto, há o apoio institucional, a estrutura de *software* e física que as partes podem fazer uso, sendo o suporte da câmara de arbitragem de caráter administrativo. Entretanto, pode editar medidas jurisdicionais, como decisões preliminares sobre a validade da convenção de arbitragem.

Salienta-se que a câmara de arbitragem consiste em uma pessoa jurídica que presta serviços de organização e administração do procedimento arbitral, assim como de definição de regras para a arbitragem sob sua gestão[14]. Dentro das funções, se apresenta a custódia dos dados do procedimento arbitral, já que funciona, muitas vezes, como uma intermediária entre os participantes, seja para a comunicação, protocolos ou recebimento de documentos.

É permitido o processamento de dados pessoais para o exercício regular do direito na arbitragem, inclusive de dados sensíveis, com base nos art. 7°, VI e 11, II, d, da LGPD, que deve se dar em conformidade com a lei em questão. Por conseguinte, é possível o

---

[13] FICHTNER, Jose Antonio; MANNHEIMER, Sérgio Nelson; MONTEIRO, André Luís. **Teoria Geral da Arbitragem.** Rio de Janeiro: Forense, 2019, p. 89.

[14] NUNES, Thiago M.; SILVA, Eduardo; GUERREIRO, Luís Fernando. **O Brasil como sede de arbitragens internacionai**s: a capacitação técnica das câmaras arbitrais brasileiras. Revista de Arbitragem e Mediação, ano 9, v. 34. São Paulo: RT, jul/set de 2012.

processamento de ambos, assim como seu armazenamento enquanto for necessário, pelas câmaras de arbitragem, que devem cumprir com o dever de proteção e com a confidencialidade.

Como mencionado anteriormente, o art. 43 da lei em tela exclui a responsabilidade civil nos casos em que há o processamento de dados em conformidade com a normativa. Neste passo, é necessária a adoção de uma política de proteção de dados pelas câmaras arbitrais, em conformidade com o art. 46, abordado anteriormente.

O ICCA, junto com a *International Bar Association* (IBA), está elaborando um protocolo de proteção de dados, à luz do GDPR, que ainda está na fase de consulta ao público[15]. Contudo, já se pode verificar a preocupação com a obediência a algumas questões: o consentimento dos envolvidos na coleta e no processamento; a necessidade de notificação quanto ao vazamento; a transparência quanto às políticas de proteção de dados da câmara arbitral; aplicação da proteção de dados na produção documental. Tais preocupações estão de acordo com a Lei Geral de Proteção de Dados e devem ser consideradas em face da aplicação extraterritorial do GDPR, que não especifica sobre sua aplicação ou não ao procedimento arbitral.

2.2. CIBERSEGURANÇA NA ARBITRAGEM

Em 2015, a Corte Permanente de Arbitragem de Haia experenciou ataques de *hackers* ao seu website, por questões relativas à disputa entre China e Filipinas, em que se debatia o mar territorial do Sul da China e os avanços da China na área sob o território filipino[16]. A Corte não se pronunciou quanto à origem do ataque, mas uma firma estadunidense, *ThreatConnect*, atribui os ataques a alguém na China. O site foi infectado com um *malware* de *hackers* chineses, que afetou, inclusive, os dispositivos dos visitantes[17].

Mediante o caso se evidenciou a vulnerabilidade também das câmaras arbitrais frente a ataques cibernéticos e falhas de segurança, o que afeta diretamente a confidencialidade dos procedimentos arbitrais. Como é cediço, uma das principais características da arbitragem, e um dos seus grandes atrativos, é o sigilo das informações relativas à controvérsia e a sua resolução[18].

---

[15] IBA. **Cybersecurity Guidelines**. []:IBA's Presidential Task Force on Cybersecurity, outubro de 2018.
[16] BLOOMBERG. 'Chinese cyberspies' hack international court's website to fish for enemies in South China Sea dispute. **South China Morning Post**. Publicado em 16 de outubro de 2015. Disponível em: <https://www.scmp.com/news/china/policies-politics/article/1868395/chinese-cyberspies-hack-international-courts-website>. Acesso em 26 de setembro de 2020.
[17] BLOOMBERG. 'Chinese cyberspies' hack international court's website to fish for enemies in South China Sea dispute. **South China Morning Post**. Publicado em 16 de outubro de 2015. Disponível em: <https://www.scmp.com/news/china/policies-politics/article/1868395/chinese-cyberspies-hack-international-courts-website>. Acesso em 26 de setembro de 2020.
[18] FOUCHARD, F.; GAILLARD, E.; GOLDMAN, B. **Fouchard Gaillard Goldman on International Commercial Arbitration**. Haia: Kluwer, 1999, p. 612.

A arbitragem atualmente se utiliza bastante da internet, principalmente, para as comunicações entre os participantes e armazenamento do processo. Com a pandemia de COVID-19, a via online se tornou a única alternativa possível, em face do isolamento social, sendo necessário a adaptação para o meio virtual e as novas demandas de segurança cibernética.

A cibersegurança ou segurança cibernética consiste nos mecanismos de tecnologia de informação e de comunicação (TIC) voltados para a proteção de informação e de dados eletrônicos[19]. Deste modo, envolve uma série de *softwares*, criptografias e plataformas para prevenir vazamentos de dados e falhas de segurança.

Diante da sociedade da informação, da necessidade de proteção de dados pessoais e da possibilidade de falhas de segurança foi criado um grupo de trabalho conjunto, formado por *New York City Bar Association* (NYC Bar), *International Institute for Conflict Prevention and Resolution* (CPR) e *International Council for Commercial Arbitration* (ICCA), para estudar a cibersegurança na arbitragem internacional e criar guias e diretrizes[20]. Em 2018, o grupo liberou um esboço de protocolo para consulta, que, depois de discussões e aprimoramentos, resultou no *ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration* de 2020, lançado em 2020.

O documento consiste em um guia de cibersegurança para a arbitragem internacional, trazendo informações e medidas para os procedimentos arbitrais, seus administradores e participantes sobre riscos, segurança e formas de diminuir tais riscos envolvidos, a partir de uma série de princípios e de seus comentários[21]. Com isto, lista quatro propósitos do protocolo, os quais são: informações sobre segurança; gestão de riscos; segurança como forma de trazer mais confidencialidade; função dos participantes na mitigação de riscos[22].

Conforme os princípios 2 e 3, todos os envolvidos devem ser informados sobre as práticas de segurança e devem segui-las. Para a escolha dos mecanismos de segurança, deve ser feito o mapeamento de risco; verificação da infraestrutura e capacidade de partes, árbitros e

---

[19] FUTURE. Arbitration leaks: a segurança da informação no procedimento arbitral. **Jota**. Publicado em 24 de abril de 2018. Disponível em: < https://www.future.com.br/arbitration-leaks-a-seguranca-da-informacao-no-procedimento-arbitral/>. Acesso em 26 de setembro de 2020.

[20] ICCA, NYC BAR, CPR. **Draft cybersecurity protocol for international arbitration**. Nova Iorque: International Council for Commercial Arbitration, New York City Bar Association, and International Institute for Conflict Prevention and Resolution (CPR), 2018.

[21] ICCA, NYC BAR, CPR. ICCA-NYC Bar-CPR **Protocol on Cybersecurity in International Arbitration**. 2020 Edition. New York Arbitration Week special printing. Nova Iorque: International Council for Commercial Arbitration, New York City Bar Association, and International Institute for Conflict Prevention and Resolution (CPR), 2019.

[22] ICCA, NYC BAR, CPR. ICCA-NYC Bar-CPR **Protocol on Cybersecurity in International Arbitration**. 2020 Edition. New York Arbitration Week special printing. Nova Iorque: International Council for Commercial Arbitration, New York City Bar Association, and International Institute for Conflict Prevention and Resolution (CPR), 2019, v.

instituições de arbitragem; custos; valor e perfil do risco da controvérsia e eficiência do procedimento arbitral, com base no princípio 6.

Diante disto, cumpre às câmaras arbitrais a análise e o mapeamento dos riscos dos procedimentos comumente submetidos à instituição para verificar quais tipos de medidas de segurança da informação necessárias. À luz do caso entre China e Filipinas na Corte Permanente de Arbitragem, verifica-se que os casos relativos entre Estados requerem um sistema de cibersegurança mais rígido.

O princípio 7 prevê os instrumentos de segurança que podem ser adotados, os quais são: gestão de ativos; controle de acesso; criptografia; segurança da comunicação e da informação; segurança física e de ambiente; segurança das operações; gestão de incidentes de segurança das informações[23]. Tais providências, que devem ser adotados desde a primeira conferência (princípio 8), servem para diminuir os riscos de falhas de segurança e, consequentemente, mitigar possíveis vazamentos de dados.

Na mesma direção, dispõe *Cybersecurity Guidelines* da *International Bar Association* (IBA) que prevê os seguintes elementos para reduzir invasões e vazamentos de dados: atualização dos *softwares;* proteção de todos os dispositivos que acessam a rede institucional; acesso por redes de internet seguras; proteção dos e-mails institucionais; encriptação de dados e dispositivos; proteção do armazenamento em nuvem; controle de acesso[24]. Contudo, isto não impede completamente violações na segurança ou uso inadequado da internet resultando em fugas de dados, pois não se pode definir quais são as medidas capazes de evitá-los[25].

Deve-se, ademais, recordar que a arbitragem consiste em um método de resolução de conflitos pautado na autonomia de vontade das partes e seus aspectos dependem do acordo dos litigantes[26]. Neste passo, as medidas de cibersegurança para o procedimento devem ser definidas com a concordância das partes, que as custearão. Todavia, as próprias câmaras arbitrais devem ter seus mecanismos de segurança da informação e da comunicação, como forma de mitigar a responsabilidade por vazamento de dados nas arbitragens geridas, sobre as quais as partes devem ser informadas e consentir com essas. Caso as partes não estejam de

---

[23] ICCA, NYC BAR, CPR. ICCA-NYC Bar-CPR **Protocol on Cybersecurity in International Arbitration**. 2020 Edition. New York Arbitration Week special printing. Nova Iorque: International Council for Commercial Arbitration, New York City Bar Association, and International Institute for Conflict Prevention and Resolution (CPR), 2019.

[24] IBA. **Cybersecurity Guidelines**. []:IBA's Presidential Task Force on Cybersecurity, outubro de 2018.

[25] IBA. **Cybersecurity Guidelines**. []:IBA's Presidential Task Force on Cybersecurity, outubro de 2018, p. 17; MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV Editora, 2018, p. 92.

[26] CARMONA, Carlos Alberto. **Arbitragem e processo**: um comentário à Lei n. 9.307/96. São Paulo: Atlas, 2009, p. 15.

acordo, a câmara deve decidir pela não realização do procedimento para evitar falhas de segurança na sua rede institucional.

Em face da vulnerabilidade das tecnologias de informação e comunicação a ataques cibernéticos e vazamentos de dados, é essencial a elaboração de um código de conduta online para os funcionários das câmaras arbitrais, os participantes dos procedimentos e para os árbitros em caso de arbitragem institucional. Afinal, a segurança de um sistema depende também daqueles que fazem uso da rede, pois basta um dispositivo inseguro para afetar todo um sistema de segurança cibernética[27]. Nesta direção, Gabriel Junqueira[28] assevera que grande parte do risco à confidencialidade da arbitragem advém de falhas humanas, e não propriamente de problemas na tecnologia.

Ademais, requer-se um trabalho de capacitação, conscientização e educação sobre internet, acessos a sites e uso dos e-mails institucionais e dos armazenamentos em nuvem da câmara, com intuito de evitar possíveis falhas de segurança na rede institucional por utilização inadequada[29].

Sem tais medidas, a adoção de mecanismos de cibersegurança não serão suficientes para conter situações de vazamentos de dados pessoais, apenas permitem um risco controlável, dependendo da colaboração dos participantes da arbitragem para cumprir com a confidencialidade dos procedimentos [30]. Desta forma, a responsabilidade pela segurança cibernética é de todos que utilizam e acessam a rede, o que implica a amplitude da cibersegurança e o conjunto de instrumentos essenciais para garanti-la.

3. CYBERSEGURANÇA E RESPONSABILIDADE CIVIL DAS CÂMARAS ARBITRAIS

O primeiro aspecto que deve ser trabalho no presente tópico é definir se a câmara arbitral é controladora ou operadora de dados, no tocante a Lei Geral de Proteção de Dados. Cumpre

---

[27] FUTURE. **Arbitration leaks**: a segurança da informação no procedimento arbitral. Jota. Publicado em 24 de abril de 2018. Disponível em: < https://www.future.com.br/arbitration-leaks-a-seguranca-da-informacao-no-procedimento-arbitral/>. Acesso em 26 de setembro de 2020; MAGRANI, Eduardo. A internet das coisas. Rio de Janeiro: FGV Editora, 2018, p. 50.

[28] JUNQUEIRA, Gabriel Herscovici. **Arbitragem brasileira na era da informática**. Um estudo das principais questões processuais. Dissertação de mestrado apresentada na Universidade do Estado de São Paulo, janeiro de 2014, p. 164.

[29] IBA. **Cybersecurity Guidelines**. []:IBA's Presidential Task Force on Cybersecurity, outubro de 2018, p. 13.

[30] COHEN, Stephanie; MORRIL, Mark. TDM Special Issue "Cybersecurity in International Arbitration" - Introduction. **TDM** 3, 2019. Disponível e:<https://www.transnational-dispute-management.com/article.asp?key=2641>. Acesso em: 26 de setembro de 2020; JUNQUEIRA, Gabriel Herscovici. **Arbitragem brasileira na era da informática**. Um estudo das principais questões processuais. Dissertação de mestrado apresentada na Universidade do Estado de São Paulo, janeiro de 2014, p. 165.

recordar que a instituição de arbitragem realiza a administração do procedimento arbitral, coletando as informações das partes e de seus advogados, dos árbitros e demais participantes, desde o requerimento de arbitragem. Ademais, é a responsável pela intermediação da comunicação, de documentos e da relação entre os envolvidos, armazenando informações no curso do processo arbitral.

À luz do art. 5º, VI, da LGPD, o controlador é definido como pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Nesta direção, a doutrina tem se direcionado para o entendimento de que as câmaras arbitrais se inserem no conceito de controlador de dados, assim como os demais envolvidos no procedimento arbitral, diante da autonomia de vontade e da confidencialidade da arbitragem[31]. Consequentemente, será essencial que a câmara se atente as diretrizes da LGPD, embora os arts. 7°, VI e 11, II, d, da LGPD, excepcionem o consentimento nos casos de processamentos de dados pessoais e sensíveis no processo arbitral.

Sendo assim, a LGPD determina deveres que devem ser cumpridos e observados pelos agentes de tratamento. As câmaras arbitrais, enquanto controladoras, devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse, hipótese de despensa de consentimento (art. 37, LGPD), sendo sempre norteados pelos princípios basilares da legislação, como a finalidade e transparência. Além disso, a Autoridade Nacional de Proteção de Dados (ANPD) poderá determinar ao controlador que elabore relatório de impacto, inclusive de dados sensíveis, referente a suas operações de tratamento, observados os segredos comercial e industrial (art. 38, LGPD), contendo requisitos como os tipos coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações, entre outros.

No que concerne a hipótese de um incidente de segurança, um destaque é o dever de reporte, onde a câmara arbitral deverá comunicar à autoridade nacional e ao titular a ocorrência que possa acarretar risco ou dano relevante aos titulares. A comunicação, além de dever ser feita em um prazo razoável, deverá conter como requisitos mínimos a descrição da natureza dos dados pessoais afetados, as informações sobre os titulares envolvidos, a indicação das medidas técnicas e de segurança utilizadas para sua proteção, observados os segredos comercial e industrial, os riscos relacionados ao incidente, os motivos da demora, no caso de a comunicação

[31]FRAZÃO, Ana (palestra). **Arbitragem e proteção de dados**. Câmara de Arbitragem da Federasul, online, 27 de agosto de 2020; IBA. **Cybersecurity Guidelines**. []:IBA's Presidential Task Force on Cybersecurity, outubro de 2018; PAISLEY, Kathleen. **It's All About the Data**: The Impact of the EU General Data Protection Regulation on International Arbitration, Fordham International Arbitration and Mediation, Conference Issue, v. 41, I. 4, 2018, pp. 869-870.

não ter sido imediata, por fim, as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo (art. 38, § 1º da LGPD).

Ao ser informada, a ANPD verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, como ampla divulgação do fato em meios de comunicação, que pode gerar um dano reputacional irreparável, e medidas para reverter ou mitigar os efeitos do ocorrido.

Deve-se levar em consideração que no juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los. Sendo assim, recrudesce a adoção de um programa de governança de dados estruturado, assim como, a adoção de medidas de segurança, como visto no tópico anterior.

A LGPD prevê que os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares, devendo o plano de resposta a incidentes e remediação deve fazer parte do programa de governança. Normas de segurança da informação, procedimento de *backup* e *restore* de descarte seguro são apenas algumas medidas que devem ser desenvolvidas e vão em consonância ao protocolo de cibersegurança e de proteção de dados pessoais para as câmaras arbitrais.

Uma alternativa promissora para mitigação dos riscos em caso de incidente de segurança é a da anonimização, que consiste na utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. Em outras palavras, significa que nenhuma informação da qual a pessoa a quem os dados se relacionam possa ser identificada de qualquer forma[32]. Desse modo, os dados anônimos não são mais considerados dados pessoais, exceto quando o processo for revertido por meios próprios ou com um esforço razoável. As técnicas mais utilizadas são a supressão, a generalização, a randomização e, por fim, a pseudonimização.

Essa última, consiste no tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro. Assim, os dados pseudonimizados podem ser anonimizados destruindo a chave.

---

[32] White paper: **EXIN Privacy & Data Protection Foundation and Essentials**.

No contexto do procedimento arbitral, essas técnicas se apresentam ainda mais relevância frente ao princípio da confidencialidade, possibilitando maior segurança jurídica, principalmente no que diz respeito à redução de risco do vazamento de informações.

Em relação à responsabilidade, por se encaixar na figura do agente de tratamento de dados, as hipóteses previstas na legislação de proteção de dados apresentadas anteriormente se aplicam, cabendo sanções judiciais e administrativas. Em relação aos demais diplomas e previsões legais na arbitragem, observa-se que o protocolo da ICCA, NYC Bar e CPR não aborda a temática da responsabilidade civil sobre falhas de segurança de informação, deixando a cargo das jurisdições nacionais a definição a respeito. E deve-se destacar que a possibilidade de responsabilidade civil relativo a esta questão não se limita apenas às câmaras arbitrais, podendo ser analisada a partir das partes, dos árbitros ou, inclusive, dos demais participantes da arbitragem. Contudo, o objetivo do artigo centra-se nas instituições de arbitragem e, consequentemente, na arbitragem institucional.

O protocolo da ICCA, NYC Bar e CPR reconhece a autoridade do tribunal arbitral para avaliar as medidas de segurança inicialmente adotadas, por iniciativa das partes ou da instituição de arbitragem, e averiguar a necessidade de novas providência de cibersegurança, nos termos do princípio 12[33]. Inclusive, o próprio painel pode alocar custos e ainda impor sanções as partes em caso de falhas na segurança das informações (princípio 13)[34]. Ou seja, o tribunal arbitral pode verificar a responsabilidade sobre vazamento de dados e, inclusive, passar para responsabilização e sanção.

Como visto, a responsabilidade civil do controlador estará constada quando causar dano patrimonial ou moral a outrem na sua atividade de processamento e haverá a necessidade de reparação, com base no art. 42, da LGPD. Todavia, será excluída a responsabilidade se provar que realizou o tratamento da forma devida, em conformidade com a LGPD, ou que é caso de culpa exclusiva do titular dos dados ou de terceiro (art. 43).

Para se inserir nos casos de exclusão, a câmara arbitral deve se utilizar dos mecanismos vistos no tópico anterior de segurança cibernética e de segurança de informação e de comunicação, demonstrando que fez o devido tratamento dos dados e que tomou as medidas

---

[33] ICCA, NYC BAR, CPR. ICCA-NYC Bar-CPR **Protocol on Cybersecurity in International Arbitration**. 2020 Edition. New York Arbitration Week special printing. Nova Iorque: International Council for Commercial Arbitration, New York City Bar Association, and International Institute for Conflict Prevention and Resolution (CPR), 2019.

[34] ICCA, NYC BAR, CPR. ICCA-NYC Bar-CPR **Protocol on Cybersecurity in International Arbitration**. 2020 Edition. New York Arbitration Week special printing. Nova Iorque: International Council for Commercial Arbitration, New York City Bar Association, and International Institute for Conflict Prevention and Resolution (CPR), 2019.

necessárias para evitar vazamentos. Atenta-se que, caso o vazamento seja resultado de invasão ou de culpa de terceiros – como as próprias partes, a instituição será isenta de responsabilidade. Contudo, é essencial que a câmara elabore um sistema de *compliance* de dados e que os envolvidos na arbitragem institucional se comprometam com esse, sob o risco de afetar toda a rede de proteção da instituição.

Diante do trabalhado anteriormente, a IBA, na sua guia de segurança cibernética, aconselha a adoção pelos escritórios de advocacia e câmaras arbitrais de seguros para casos de falhas na segurança, seja esta causada por disfunções do sistema de cibersegurança ou por falha humana, e de vazamento de dados[35]. Deste modo, a seguradora responde pelas situações em questão.

Por conseguinte, é aconselhável a elaboração de um programa de *compliance* de dados, como defendido, e de um sistema de segurança cibernética, com a capacitação e conscientização de todos que acessam a rede institucional e fazem uso dos e-mails e armazenamento de dados da câmara arbitral. Mediante tais medidas, a instituição de arbitragem, nas arbitragens institucionais, exclui a responsabilidade em casos de vazamentos de dados pessoais e de dados dos procedimentos arbitrais. Ademais, é imprescindível a adoção de seguro para os casos em questão, considerando a falibilidade humana e tecnológica.

CONSIDERAÇÕES FINAIS

A LGPD dispõe especificamente sobre o procedimento arbitral e exclui a necessidade de consentimento para o processamento dos dados pessoais e sensíveis imprescindíveis para o processo. Independentemente desta disposição, os envolvidos, como controladores de dados, devem atentar aos princípios e deveres previstos na legislação em seu processamento, sob pena de responsabilidade civil.

Neste cenário, a câmara arbitral, nas arbitragens institucionais, atua na administração do procedimento arbitral, processando dados pessoais dos envolvidos desde o momento do requerimento de arbitragem. Adicionalmente, concentra um intenso fluxo de dados na intermediação das comunicações, no recebimento de documentos, no suporte das conferências e na produção documental.

Diante desta situação, as instituições internacionais dedicadas ao estudo da arbitragem editaram guias e diretrizes para auxiliar os participantes da arbitragem frente à regulação da

[35] IBA. **Cybersecurity Guidelines**. []:IBA's Presidential Task Force on Cybersecurity, outubro de 2018, p. 17.

proteção de dados. É cediço que o instituto requer, em diversos procedimentos, o dever de confidencialidade, o que torna a relevância da salvaguarda de dados ainda maior.

Neste passo, surge a preocupação com o consentimento dos envolvidos, a transparência, as políticas de proteção de dados e a adoção de sistemas de segurança de informação. Sendo a maioria das comunicações, armazenamentos e intercâmbio de informações realizadas virtualmente, faz-se imprescindível a adoção de mecanismos de segurança cibernética, como apontado pelo *ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration*. O documento prevê a tomada de diversas medidas de segurança e de regras de conduta para os envolvidos na arbitragem. Com isto, a câmara deve buscar as providências de cibersegurança e de segurança da informação mais adequadas aos conflitos normalmente submetidos e informar devidamente a estes sobre as políticas de dados e a necessidade de respeito a elas.

Por meio da adoção destes mecanismos, a câmara arbitral adentra nas hipóteses previstas no art. 43, da LGPD de exclusão da responsabilidade civil e cumpre devidamente a legislação em questão, protegendo os dados dos envolvidos e sua rede institucional.

REFERÊNCIAS

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

BARROS, Vera Cecília M. **A importância do secretário da arbitragem**, pp. 363-386. *In:* CARMONA, Carlos Alberto; LEMES, Selma Ferreira; MARTINS, Pedro Batista (Coord.). 20 anos da Lei de Arbitragem São Paulo: Atlas, 2017.

BLOOMBERG. '**Chinese cyberspies' hack international court's website to fish for enemies in South China Sea dispute**. South China Morning Post. Publicado em 16 de outubro de 2015. Disponível em: <https://www.scmp.com/news/china/policies-politics/article/1868395/chinese-cyberspies-hack-international-courts-website>. Acesso em 26 de setembro de 2020.

CAPANEMA, Walter Aranha. **A responsabilidade civil da Lei Geral de Proteção de Dados**. Cadernos Jurídicos da Escola Paulista da Magistratura, ano 21, nº 53. São Paulo. 2020, P. 163-170. Disponível em: <http://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_6_a_responsabilidade_civil.pdf?d=637250347559005712>. Acesso em: 27 set. 2020.

CARMONA, Carlos Alberto. **Arbitragem e processo**: um comentário à Lei n. 9.307/96. São Paulo: Atlas, 2009.

CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz e Terra, 1999.

COHEN, Stephanie; MORRIL, Mark. **TDM Special Issue "Cybersecurity in International Arbitration" - Introduction**. TDM 3, 2019. Disponível e:<https://www.transnational-dispute-management.com/article.asp?key=2641>. Acesso em: 26 de setembro de 2020.

CONCERINO, Arthur José. **Internet e segurança são compatíveis?** *In:* LUCCA, Newton de; SIMÃO FILHO, Adalberto (Coord.). Direito e internet: Aspectos jurídicos relevantes. 2 ed. São Paulo: Quartier Latin, 2005, pp. 153-178.

DOMINGOS, Pedro. **The master algorithm:** how the quest for the ultimate machine learning will remake our world. Nova York: Basic Books, 2015.

FICHTNER, Jose Antonio; MANNHEIMER, Sérgio Nelson; MONTEIRO, André Luís. **Teoria Geral da Arbitragem**. Rio de Janeiro: Forense, 2019.

FOUCHARD, F.; GAILLARD, E.; GOLDMAN, B. **Fouchard Gaillard Goldman on International Commercial Arbitraion.** Haia: Kluwer, 1999.

FRAZÃO, Ana (palestra). **Arbitragem e proteção de dados.** Câmara de Arbitragem da Federasul, online, 27 de agosto de 2020.

FUTURE. **Arbitration leaks**: a segurança da informação no procedimento arbitral. Jota. Publicado em 24 de abril de 2018. Disponível em: < https://www.future.com.br/arbitration-leaks-a-seguranca-da-informacao-no-procedimento-arbitral/>. Acesso em 26 de setembro de 2020.

HAN, Byung-Chul. **Sociedade da transparência**. Petrópolis, RJ: Vozes, 2017.

IBA. **Cybersecurity Guidelines**. []:IBA's Presidential Task Force on Cybersecurity, outubro de 2018.

ICCA, NYC BAR, CPR. **Draft cybersecurity protocol for international arbitration. N**ova Iorque: International Council for Commercial Arbitration, New York City Bar Association, and International Institute for Conflict Prevention and Resolution (CPR), 2018.

ICCA, NYC BAR, CPR. **ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration**. 2020 Edition. New York Arbitration Week special printing. Nova Iorque: International Council for Commercial Arbitration, New York City Bar Association, and International Institute for Conflict Prevention and Resolution (CPR), 2019.

JUNQUEIRA, Gabriel Herscovici**. Arbitragem brasileira na era da informática**. Um estudo das principais questões processuais. Dissertação de mestrado apresentada na Universidade do Estado de São Paulo, janeiro de 2014.

MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV Editora, 2018.

NUNES, Thiago M.; SILVA, Eduardo; GUERREIRO, Luís Fernando. **O Brasil como sede de arbitragens internacionais**: a capacitação técnica das câmaras arbitrais brasileiras. Revista de Arbitragem e Mediação, ano 9, v. 34. São Paulo: RT, jul/set de 2012.

PAISLEY, Kathleen. **It's All About the Data**: The Impact of the EU General Data Protection Regulation on International Arbitration, Fordham International Arbitration and Mediation, Conference Issue, v. 41, I. 4, 2018, pp. 836-841.

PINHEIRO, Patricia Peck. **Direito digital.** 5. ed. rev.atual. e ampl. de acordo com as Leis n. 12.735 e 12.737de 2012.São Paulo : Saraiva, 2013.

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

SCHNEIDER, M. E; KUNER, C. **Dispute resolution in international electronic commerce.** Journal of International Arbitration, v. 14, n. 3, Kluwer, setembro de 1997, pp. 5-38.

INTELIGÊNCIA ARTIFICIAL E ADVOCACIA

Luis Eduardo de Souza Leite Trancoso Daher [36]
Rafaela Gonçalves Duque[37]

INTRODUÇÃO

Ab initio, salienta-se que a expressão "Inteligência Artificial (IA)" se refere a um conceito um tanto quanto abstrato e de difícil definição, mas pode-se inferir que esta se relaciona com o ramo da computação e se define como os esforços para se chegar o mais próximo possível de uma inteligência orgânica, como a dos seres humanos.

O pressuposto de imitar as funções cognitivas humanas concede à IA uma polivalência de temas em seu escopo, interseccionando as mais variadas áreas do conhecimento, tornando a Inteligência Artificial multifacetada. Por sua característica multidisciplinar, a IA pode ser aplicada no mundo jurídico, favorecendo a otimização de processos, redução de custos, aumento da produtividade e melhora dos resultados obtidos.

A partir desse viés, contextualiza-se que, anualmente, milhões de ações são ajuizadas no Brasil[38]. Essa judicialização em massa implica verdadeiro congestionamento do sistema judiciário e, por conseguinte, uma maior lentidão nas decisões a serem tomadas.

Isto porque, o enorme volume de informações associadas aos processos judiciais acaba comprometendo a efetividades do trabalho dos operadores do direito que, como seres humanos que são, possuem limitações cognitivas para lidar com o excesso de demanda no judiciário[40].

Sendo assim, o expressivo número de ações, tramitando nos mais diversos tribunais do país, demonstra uma grande necessidade de buscar soluções e mecanismos tecnológicos que

[36] Graduando em Direito pela Universidade Federal Fluminense (Niterói – Rio de Janeiro, Brasil), E-mail: luiseduardodaher@id.uff.br , http://lattes.cnpq.br/6797039743684964.
[37] Graduanda em Direito pela Universidade Federal Fluminense (Niterói – Rio de Janeiro, Brasil) , E-mail: rafaeladuque@id.uff.br, http://lattes.cnpq.br/2172596164396764.
[38] FELIPE, Bruno Farage da Costa; PERROTA, Raquel Pinto Coelho. **Inteligência Artificial no Direito**: Uma realidade a ser desbravada. Revista de Direito, Governança e Novas Tecnologias, Salvador, v.4, n.1, p. 1-16, jan./jun. 2018.
[40] GIRARDI, Rosario. **Inteligência Artificial Aplicada ao Direito**. 1. ed. Edição do autor. Brasil: 2020, p. 8. ISBN 978-65-00-03948-1.

visem imprimir maior celeridade e economia às atividades judiciais, bem como menor dispêndio de tempo dos profissionais envolvidos[42].

Nesse sentido, a Inteligência Artificial (IA) tem sido utilizada, cada vez mais, na procura da melhora da qualidade e eficiência dos serviços jurídicos, através da construção de sistemas computacionais capazes de complementar as habilidades cognitivas dos diferentes operadores jurídicos, tornando efetivo o processo decisório[43].

Além de favorecer uma melhor compreensão dos processos cognitivos e da inteligência humana, a IA tem sido uma grande aliada na construção dos processos de raciocínio e argumentação jurídica, o que contribui para uma melhora e evolução do Direito em si, como matéria[45].

Nesse desiderato, o presente estudo busca discutir brevemente a aplicação da inteligência artificial na atividade jurídica e no mundo hiperconectado, perpassando pelas técnicas de raciocínio automatizado[47] e de representação de conhecimento[48], a fim de melhor delinear as principais aplicações práticas da IA.

Vale destacar que, sob o viés da automatização da tomada de decisões em âmbito jurídico, não se pode olvidar que muitas tarefas, antes consideradas como prerrogativas humanas, hoje são executadas por *estes* operadores autômatos.

Essa evolução tecnológica, em que *Inteligências Artificiais* e mecanismos automatizados detêm poder para tomada de decisões, nos leva a refletir sobre os efeitos desses sistemas para a autonomia pessoal e, consequentemente, sobre a necessidade de se preservar os direitos fundamentais, o que sugere a importância de recorrermos à ética como instrumento capaz de encaminhar soluções que, eventualmente, possam consolidar-se em alternativas legislativas[50], além de ressaltar a importância do direito à revisão de decisões automatizadas.

---

[42] FELIPE, Bruno Farage da Costa; PERROTA, Raquel Pinto **Coelho. Inteligência Artificial no Direito**: Uma realidade a ser desbravada. Revista de Direito, Governança e Novas Tecnologias. Salvador: Organização Comitê Científico, 2018, v.4, p.2.

[43] GIRARDI, Rosario. Inteligência Artificial Aplicada ao Direito. 1. ed. Edição do autor. Brasil: 2020, p. 3. ISBN 978-65-00-03948-1.

[45] GIRARDI, Rosario. Inteligência Artificial Aplicada ao Direito. 1. ed. Edição do autor. Brasil: 2020, p. 8-9. ISBN 978-65-00-03948-1.

[47] Segundo a Autora Rosario Girardi, o raciocínio automatizado visa a construção de sistemas de computação que automatizam o processo cognitivo. O termo foi, tradicionalmente, associado ao raciocínio dedutivo como praticado em matemática e lógica formal. Existem quatro tipos principais de raciocínio: dedução, indução, abdução e analogia.

[48] As linguagens de representação de conhecimento, como a lógica formal, são utilizadas para representar computacionalmente as regras de inferência do processo de raciocínio.

[50] DONEDA, D.C.M.; MENDES, L.S.; SOUZA, C.A.P.; ANDRADE, N.N.G. Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. Pensar: Revista de Ciências Jurídicas, Fortaleza, v.23, n.4, p. 1-17, out./dez.2018.

Por derradeiro, o estudo, além de abordar as aplicações práticas da IA no mundo jurídico, irá discorrer sobre a ética e a Proteção de Dados Pessoais como instrumentos de salvaguarda dos direitos fundamentais, tendo em vista a prática automatizada das decisões dos operadores do direito e o iminente risco de serem violadas as garantias constitucionais do *due processo of law*[51], como igualdade, publicidade e segurança jurídica.

Assim, a artigo será organizado da seguinte forma: em um primeiro momento, serão levantadas algumas considerações iniciais sobre a Inteligência Artificial e a sua relação próxima com os dados. Posteriormente, será abordada a importância da ética na regulação da IA. Em sequência, teremos como ponto focal as principais aplicações da IA no Direito, sob a luz das técnicas de raciocínio automatizado e representação do conhecimento. Por fim, teremos as conclusões do estudo e uma breve discussão sobre os desafios ainda existentes na aplicação da IA no mundo jurídico.

1. O INÍCIO DE TUDO

Quando se trata de Inteligência Artificial, abordar a face histórica desta discussão e a maneira como este conceito se ramifica atualmente é essencial para compreendermos seus desdobramentos multidisciplinares. Em 1943, Warren McCulloch e Walter Pitts apresentaram um artigo que falava pela primeira vez no conceito de redes neurais, estruturas de raciocínio artificiais que imitam o nosso sistema nervoso, com seus nós interconectados funcionam justamente como os neurônios humanos, sendo um bom pontapé inicial para a IA[52].

Em 1950, Alan Turing desenvolveu uma forma de avaliar se uma máquina consegue se passar por um humano em uma conversa por escrito. Denominado teste de Turing, originalmente conhecido como Jogo da Imitação, o experimento deu título ao filme que retratou a vida do pesquisador, além de representar um marco para a ciência no ramo das IA's[54].

A primeira vez que se falou sobre Inteligência Artificial, como um campo de estudo acadêmico, foi em 1956, em uma conferência em Darthmouth College, uma universidade estadunidense. O termo cunhado por John McCarthy caiu como uma luva para esta matéria que

---

[51] Princípio fundamental do processo civil, previsto na Constituição da República Federativa do Brasil de 1988, em seu art. 5º, inciso LIV. A partir desse princípio decorrem todas as consequências processuais que garantiriam aos litigantes o direito a um processo e uma sentença justa.

[52] FRAZÃO, Ana; MULHOLLAND, Caitlin; Inteligência Artificial e Direito: ética, regulação e responsabilidade. 1ª ed. São Paulo: Thomson Reuters Brasil, 2019. p. 41.

[54] CARNEIRO, Tayná; FALCÃO, Cintia Ramos. Direito Exponencial: o papel da Novas Tecnologias no Jurídico do Futuro. 1ª ed. São Paulo: Thomson Reuters Brasil, 2020. P. 337.

foi impulsionada a partir da segunda guerra mundial, tendo nomes como Allan Turing, Ada Lovelace, Herbert Simon e o próprio John McCarthy como principais idealizadores[55].

Para entendermos suas aplicações práticas, precisamos realizar um esforço no sentido de categorizar a IA, de entendermos que não existe pura e simplesmente um único tipo de Inteligência Artificial, e sim diversas ramificações desta matéria. Devemos, portanto, levar em conta a existência de três grandes grupos: Inteligência Artificial Limitada (ANI), Inteligência Artificial Geral (AGI) e Superinteligência (ASI)[56].

A ANI ou "IA Fraca" (*Weak AI*) é caracterizada por ser o tipo mais básico de IA, é o nível mais baixo, que consegue apenas se especializar em uma área específica, como a emblemática IA jogadora de Xadrez, por exemplo. Essa categoria se subdivide ainda em **Máquinas Reativas**, que literalmente somente reagem às situações, não possuem nenhuma capacidade de memória e aprendizado com situações passadas, e IA's de **Memória Limitada**, que dizem respeito às máquinas que conseguem processar situações passadas (memória) para fundamentar a decisão atual[57].

Um exemplo que já estamos ficando acostumados a ver são os carros autônomos, eles observam a velocidade e a direção dos outros carros para decidirem o que fazer, além disso, aprendem com os erros que outros carros autônomos, que estejam interligados ao seu sistema, cometeram anteriormente[58].

Já a AGI, conhecida como "IA Forte" (*Strong AI*) ou "IA nível humano", relaciona-se a uma Inteligência artificial que possui domínio e *expertise* em diversas áreas, não mais se limitando a apenas uma específica. Esta IA se equivaleria à capacidade intelectual e multidisciplinaridade do ser humano e passaria com facilidade no Teste de Turing, relatado anteriormente. Este tipo de Inteligência Artificial ainda não foi concebido, continua objeto exclusivo das obras de ficção científica e, assim como a anterior, é subdividida em dois grupos, que segundo Martha Gabriel são[59]:

> – **Máquinas Cientes**: classe de mentes computacionais que não apenas "enxergam" o mundo (criam representações), mas também conseguem "perceber" outros agentes ou entidades – elas compreendem que as pessoas, criaturas e objetos no mundo podem ter pensamentos e emoções que precisam ser consideradas para ajustar o seu próprio

[55] FEIGELSON, Bruno; MALDONADO, Viviane Nóbrega. Advocacia 4.0. 1ª ed. São Paulo: Thomson Reuters Brasil, 2019. p.75.
[56] GABRIEL, Martha. Você, Eu e os Robôs: Pequeno Manual do Mundo Digital. 1ª ed. São Paulo: Atlas, 2018. p. 188-190.
[57] GABRIEL, Martha. Você, Eu e os Robôs: Pequeno Manual do Mundo Digital. 1ª ed. São Paulo: Atlas, 2018. p. 188-190.
[58] GABRIEL, Martha. Você, Eu e os Robôs: Pequeno Manual do Mundo Digital. 1ª ed. São Paulo: Atlas, 2018. p. 188-190.
[59] GABRIEL, Martha. Você, Eu e os Robôs: Pequeno Manual do Mundo Digital. 1ª ed. São Paulo: Atlas, 2018. p. 188-190.

> comportamento (ciência). Essas habilidades são essenciais para permitirem interações sociais, e é a partir delas que os humanos formaram sociedades – seria muito difícil, ou mesmo impossível, trabalharmos juntos sem compreender as motivações e intenções uns dos outros, e sem considerar o que o outro sabe sobre si e o ambiente.
> – **Máquinas Autoconscientes**: essa classe de sistemas de IA vai além na Teoria da Mente e possui "autoconsciência". Em outras palavras, elas têm consciência não só sobre o seu exterior, mas também sobre si mesmas. Essa é uma diferença grande em relação a ter ciência apenas do que está do lado de fora – seres autoconscientes conhecem os seus estados internos, e são capazes de prever os sentimentos dos outros. Por exemplo, nós pressupomos que alguém que está chorando está triste porque, quando estamos tristes, nós choramos. Da mesma forma que a inteligência, a consciência é algo difícil de se definir, mas que conseguimos facilmente reconhecer[60].

Por fim, há ainda a Superinteligência (ASI), que compreende desde computadores um pouco mais inteligentes e desenvolvidos em áreas como criatividade científica, conhecimentos gerais e habilidades sociais até aqueles que podem ser milhões de vezes melhores do que nós. Esse é o conceito principal de Inteligência Artificial que perambula pelo universo cinematográfico e literário, discorrendo até mesmo sobre a possibilidade da Singularidade Tecnológica, uma hipótese em que as mudanças paradigmáticas da história humana correlacionadas com o desenvolvimento desenfreado de tecnologias relacionadas à Superinteligências Artificiais culminariam inevitavelmente na extinção da raça humana[61].

2. OS DADOS E A INTELIGÊNCIA ARTIFICIAL

Em perspectivas mais contemporâneas e realistas, é necessário que tenhamos consciência de que a Inteligência Artificial se manifesta de forma mais palatável e concebível a partir do nascimento da internet, a partir do momento em que começamos a digitalizar nossas vidas. Há um fenômeno no meio dessa realidade digital, dessa sociedade da informação, que atua como marco impulsionador da IA e de tantas outras tecnologias atualmente: o "*Big Data*".

A internet surge como um dos melhores métodos para se gerar e armazenar dados e, conforme a tecnologia avança, essa possibilidade de gerar, armazenar e gerenciar dados aumenta. À medida em que se expandem os HD's[62] e a velocidade de transferência da internet aumenta, mais combustível é injetado no tanque da "*Big Data"* e maior e de mais qualidade é o banco de dados amostrais que pode ser utilizado para aprimorar a IA[63].

---

[60] GABRIEL, Martha. Você, Eu e os Robôs: Pequeno Manual do Mundo Digital. 1ª ed. São Paulo: Atlas, 2018. p. 188-190.
[61] GABRIEL, Martha. Você, Eu e os Robôs: Pequeno Manual do Mundo Digital. 1ª ed. São Paulo: Atlas, 2018. p. 188-190.
[62] Os Hard Disks ou simplesmente HD's são unidades de armazenamentos de dados muito comuns em computadores e notebooks.
[63] MAGRANI, Eduardo. Entre Dados e Robôs: Ética e Privacidade na Era da Hiperconectividade. 2ª ed. Porto Alegre: Arquipélago Editorial, 2019. p.22-24.

Neste sentido, podemos e devemos caracterizar o *Big Data* como um fenômeno intrínseco ao mundo hiperconectado em que estamos cada vez mais inseridos. É importante destacar que além da internet, que funcionou como um facilitador da proliferação e consequente criação de mais dados no mundo, precisamos conceituar e dar o devido destaque também à Internet das Coisas (*Internet of Things – IOT*) que já mudou o paradigma de captação e armazenamento de dados[64].

Não há um conceito específico definido para Internet das Coisas, mas podemos dizer que ela consiste na interconexão de objetos ordinários, de modo que estes objetos formam uma enorme rede de dispositivos que interagem entre si, captando, analisando e gerando dados. No âmbito da *IOT*, há a presença de três conceitos elementares para seu funcionamento: conectividade, uso de sensores/atuadores e capacidade computacional de processamento e armazenamento de dados. Podemos citar como exemplo a pulseira inteligente que conta seus passos e transfere para o aplicativo de saúde do seu celular, tudo através da internet. Neste delinear e com o avanço da Internet das Coisas, estima-se um fluxo de dados ainda maior para o futuro[65].

Neste cenário de abundância de dados é necessário designar alguns esforços para gerir e organizar este amontoado, sendo este acontecimento, como já mencionamos, denominado de *Big Data*, um efeito cascata do mundo digitalizado, caracterizado justamente pela inconcebível quantidade de dados gerada e a capacidade de se ordenar dentro deste espectro[66].

Por intermédio do fenômeno da digitalização e datificação[67] da vida, passamos a vivenciar um paradigma da necessidade de criação de novos direitos fundamentais, além da reinterpretação daqueles que já existiam, sob a lente tecnológica da sociedade conectada. É nesta linha de raciocínio que se discute o direito à Proteção dos Dados Pessoais, como uma extensão lógica dos direitos personalíssimos à intimidade, vida privada, honra e imagem dos indivíduos, trazidos pelo inciso X do artigo 5º da Constituição da República Federativa do Brasil[68].

---

[64] MAGRANI, Eduardo; Entre Dados e Robôs: Ética e Privacidade na Era da Hiperconectividade. 2ª ed. Porto Alegre: Arquipélago Editorial, 2019. p.22-24.
[65]MAGRANI, Eduardo. Internet das Coisas. 1ª ed. Porto Alegre: FGV Editora, 2018. p. 20
[66] MAGRANI, Eduardo. Entre Dados e Robôs: Ética e Privacidade na Era da Hiperconectividade. 2ª ed. Porto Alegre: Arquipélago Editorial, 2019. p.22-24.
[67] Datificação é a transformação de nossas vidas em dados computadorizados, ou seja, é a representação eletrônica de nossas fotos, vídeos, gostos, comportamentos e costumes, que criam versões abstratas de nós por meio das tecnologias da informação, que tem o potencial de refletir concretamente no mundo físico.
[68] CARNEIRO, Tayná; FALCÃO, Cintia Ramos. Direito Exponencial: o papel da Novas Tecnologias no Jurídico do Futuro. 1ª ed. São Paulo: Thomson Reuters Brasil, 2020. p. 469-470

Um embate entre o direito à Proteção de Dados Pessoais e as tão discutidas Inteligências Artificiais, que se alimentam e utilizam como base conjuntos de dados, era uma consequência previsível. Em alguns aspectos estes conceitos se cruzam, entretanto, nos interessa somente o direito a revisão de decisões automatizadas derivado da proteção de dados e da utilização, cada vez mais corriqueira, de mecanismos de IA em tribunais, bancos de análise de crédito e qualquer outro ambiente que envolva decisões automatizadas na prática.

Um dos institutos mais importantes e presentes no campo da IA e das tomadas de decisões autônomas é o de *Machine Learning*[69] (ML), que basicamente se traduz em um algoritmo[70] com capacidade para interpretar, criar padrões e literalmente aprender "sozinho". Claro, tudo isso com o estímulo correto, dado pelo cientista da computação, engenheiro ou qualquer pessoa que esteja alimentando uma máquina com essas características. É deste arranjo que nascem as tomadas de decisão automatizadas, realizadas por Inteligências Artificiais com capacidade de Aprendizado de Máquina[71].

Ainda sobre o *Machine Learning*, absorve-se a importante lição de Caitlin Mulholland e Isabella Z. Frajhof:

> O uso de programas de aprendizado por máquinas, conhecido pelo termo *machine learning*, permite que sejam criados sistemas de Inteligência Artificial (IA) que desenvolvem a capacidade de tomadas de decisão absolutamente autônomas em relação à interferência humana. Isto é, torna-se possível por meio de tratamento de dados em massa – *inputs* – o desenvolvimento de autoaprendizagem das máquinas – *i.e.* programas e sistemas – que permite o alcance de determinados resultados – *outputs* – independentemente de qualquer mediação por um ser humano. Ou seja, o próprio sistema alcança resultados por meio de processos dedutivos e análises estatísticas que vão sendo determinados com base em correlações realizadas pela IA. Esses resultados, em não raras vezes, são obtidos sem que seja possível, *a priori*, reconhecer os padrões adotados pela IA para a análise de dados selecionados e o modo de trabalho que levaram a esses *outputs*[72].

Quando uma máquina tem a capacidade de se orientar sozinha por meio de estruturas de *Big Data*, funcionando de maneira mais próxima ainda a um conjunto orgânico, esta recebe a alcunha de Deep Learning. Este conceito foi concebido baseado na ideia de redes neurais, se estruturando por meio da sobreposição de diversas camadas não lineares de processamento de dados, de maneira muito mais próxima ao cérebro humano[73].

---

[69] No Brasil é comumente chamado de Aprendizado de Máquina, a tradução literal de Machine Learning.
[70] Algoritmos são basicamente uma sequência de regras que mostram o passo-a-passo necessário para executar uma tarefa específica.
[71] FEIGELSON, Bruno; MALDONADO, Viviane Nóbrega. Advocacia 4.0. 1ª ed. São Paulo: Thomson Reuters Brasil, 2019. p 79.
[72] FRAZÃO, Ana; MULHOLLAND, Caitlin; Inteligência Artificial e Direito: ética, regulação e responsabilidade. 1ª ed. São Paulo: Thomson Reuters Brasil, 2019. p. 265 e 266.
[73] GABRIEL, Martha. Você, Eu e os Robôs: Pequeno Manual do Mundo Digital. 1ª ed. São Paulo: Atlas, 2018. p. 210 a 214.

Dito isto, faz-se necessária uma reflexão relacionada ao titular de dados, indivíduo que sofre as consequências da utilização de dados no processo de aprendizado de máquina. Neste seguimento, é válido destacarmos que alguns esforços já vêm sendo notados e a recém vigorada Lei Geral de Proteção de Dados traz, em seu artigo 20, o que estudiosos do assunto denominam "direito à explicação".

Este direito decorre do princípio da transparência e preceitua que o titular de dados deve ter direito à revisão de decisões tomadas exclusivamente com base na análise de dados, por mecanismos automatizados. Com isso, a legislação resguarda o direito a uma análise humanizada, que leve em conta fatores menos inteligíveis e claros para um ente que não é dotado de inteligência emocional, social e muito menos de raciocínio crítico que demande a compreensão e a interpretação de outros fatores que não sejam dados brutos[74].

O direito à revisão das decisões é pressuposto essencial para a construção de uma regulação madura e inserida em uma cultura protecional de dados pessoais, além de revelar, juntamente com as demais legislações de proteção de dados, uma inclinação à aplicabilidade do Princípio da Precaução na Regulação de Inteligência Artificial[75].

Neste seguimento, quando falamos em tomada de decisão por meio de Inteligência Artificial, precisamos considerar ainda os pressupostos para a criação e construção desse ente computadorizado. Questionamentos acerca da imparcialidade, eticidade e construção algorítmica enviesada precisam ser levantados quando discutimos o tema.

Abordar o mundo virtual de forma dissociada do real ou natural não é mais uma possibilidade. É imperioso que se admita a hibridização e a confluência destes dois espectros para que possamos debater acerca de possibilidades regulatórias que minimizem esses impactos[76].

3. ÉTICA E REGULAÇÃO

Partindo do ponto de vista de que a facilidade, a otimização de processos e as soluções de atendimento exercem um papel imprescindível no dia a dia das grandes corporações que trabalham com o público e que, em contrapartida a isso, não se almeja renunciar à proteção de

[74] FRAZÃO, Ana; MULHOLLAND, Caitlin. Inteligência Artificial e Direito: ética, regulação e responsabilidade. 1ª ed. São Paulo: Thomson Reuters Brasil, 2019. p. 265 e 266.
[75]FRAZÃO, Ana; MULHOLLAND, Caitlin. Inteligência Artificial e Direito: ética, regulação e responsabilidade. 1ª ed. São Paulo: Thomson Reuters Brasil, 2019. p. 215.
[76] DE LIMA, Ana Paula M. Canto; HISSA, Carmina Bezerra; SALDANHA, Paloma Mendes. Direito Digital: Debates Contemporâneos 1ª ed. São Paulo: Thomson Reuters Brasil, 2019. p. 23

nossos dados pessoais e do direito à privacidade e vida íntima, é premente que façamos um exercício de ponderação, no sentido de melhor balancear os interesses controvertidos.

Essa ponderação se mostra essencial para a construção de uma base regulatória robusta, que respeite o indivíduo titular de direitos, mas que não suprima ao mesmo tempo os avanços tecnológicos e os interesses empresariais benéficos à sociedade.

Em confluência com este entendimento e voltando a abordar a lógica do Princípio da Precaução, não devemos nos olvidar das lições de Bruno Ricardo Bioni e Maria Luciano, que determinam:

> O princípio da precaução fornece um substrato importante para se pensar medidas e estratégias de regulação de IA, notadamente como lidar com situações de riscos de danos ou de desconhecimento dos potenciais malefícios e benefícios desse tipo de tecnologia. A automatização de processos de tomadas de decisão, a partir do emprego de IA, não deve se constituir como um argumento ingênuo em defesa de objetividade e neutralidade. Tais circuitos decisórios carregam escolhas das entidades e pessoas envolvidas na sua construção, sendo modulado pela agenda política e aspectos socioeconômicos, de forma implícita ou explícita, que lhes são subjacentes[77].

Como destacado pelos autores, a transparência e a dita imparcialidade dos mecanismos de Inteligência Artificial podem não se revelar como exemplos a serem seguidos. A busca pela equidade de tratamento, por meio da objetividade e reflexão da realidade de uma IA, pode se mostrar um verdadeiro aparato de perpetuação de preconceitos e opressões, sob o risco de ser utilizada ainda para a preponderação de um monopólio ou até mesmo grupo político sobre o outro[78].

Neste cenário, buscando uma saída para mirar horizontes de igualdade de fato, encontra-se o princípio da *Accountability* desses sistemas, buscando não mais uma transparência literal e sem propósito, mas uma transparência qualificada, por intermédio dos relatórios de impacto à proteção de dados pessoais (RIPDP) e, acima de tudo, que ensejem ânimos de paridades de armas.

Neste ritmo de transparência qualificada para gerar igualdade qualificada, é necessário entender que um processo de regulação prematuro e que não leve em consideração a precaução e os princípios da proteção de dados, livre concorrência, não discriminação, respeito aos direitos humanos, explicabilidade, segurança e desenvolvimento tecnológico pode trazer mais riscos

---

[77] FRAZÃO, Ana; MULHOLLAND, Caitlin. Inteligência Artificial e Direito: ética, regulação e responsabilidade. 1ª ed. São Paulo: Thomson Reuters Brasil, 2019. 228

[78] CARNEIRO, Tayná; FALCÃO, Cintia Ramos. Direito Exponencial: o papel da Novas Tecnologias no Jurídico do Futuro. 1ª ed. São Paulo: Thomson Reuters Brasil, 2020. p.415-416.

aos direitos fundamentais ao vislumbrar a possibilidade de potencializar cargas e desigualdades históricas e socialmente construídas[79].

Destacadas estas considerações com relação à regulação e sua íntima relação com a ética e a matérias intrinsecamente ligadas ao direito, partimos então para uma discussão mais empírica. Em muito se correlacionam a prática da advocacia e a utilização da Inteligência Artificial no direito de uma forma geral, e dissecar esta relação é a que se destina o próximo tópico.

4. APLICAÇÕES DA INTELIGÊNCIA ARTIFICIAL NO DIREITO

Antes de adentramos ao tema, faz-se necessário destacar que a inteligência artificial não se confunde com a informática clássica aplicada ao Direito. Enquanto a informática clássica se limita a realizar tarefas ou procedimentos que já foram pré-estabelecidos pelo desenvolvedor, através da programação de algoritmos, a IA vai muito além, já que simula a inteligência humana e seus processos cognitivos, podendo inclusive ter autonomia decisória. [80]

Nesse sentido, a IA, aplicada ao mundo do direito, pode auxiliar o raciocínio jurídico, o conhecimento jurídico, a otimização de grande volume de informações processuais e, até mesmo, a hermenêutica jurídica[81].

No que tange ao raciocínio jurídico, destaca-se que os processos decisórios, geralmente, são baseados em casos concretos similares, aplicando-se a jurisprudência. Desta forma, a IA, através do uso *softwares*, pode auxiliar a tomada de decisões, à medida em que será mais efetiva a busca por jurisprudência que possa ser aplicada a um caso concreto semelhante a outro já decidido[82].

O conhecimento jurídico, disponível na forma de normas jurídicas, doutrina e jurisprudência, pode ser organizado, de maneira codificada e mapeada, pelos sistemas de computação, a fim de otimizar o trabalho jurídico[83].

No que se refere ao grande volume de informações jurídicas, salienta-se que a expansão dos conteúdos do direito; o aumento constante do volume de instrumentos normativos: leis,

---

[79] FRAZÃO, Ana; MULHOLLAND, Caitlin. Inteligência artificial e direito: ética, regulação e responsabilidade. 1ª ed. São Paulo: Thomson Reuters Brasil, 2019. p. 209-210.
[80] GIRARDI, Rosario. Inteligência Artificial Aplicada ao Direito. 1. ed. Edição do autor. Brasil: 2020, p. 8-9. ISBN 978-65-00-03948-1
[81] GIRARDI, Rosario. Inteligência Artificial Aplicada ao Direito. 1. ed. Edição do autor. Brasil: 2020, p. 38. ISBN 978-65-00-03948-1
[82] GIRARDI, Rosario. Inteligência Artificial Aplicada ao Direito. 1. ed. Edição do autor. Brasil: 2020, p. 38. ISBN 978-65-00-03948-1
[83] GIRARDI, Rosario. Inteligência Artificial Aplicada ao Direito. 1. ed. Edição do autor. Brasil: 2020, p. 38-39. ISBN 978-65-00-03948-1

decretos, portarias etc.; e a intensa mutabilidade do direito, pelas rápidas transformações sofridas pelo conteúdo dos instrumentos normativos, desafia as limitações cognitivas dos operadores humanos, daí decorrendo a importância da IA[84].

Esse demasiado volume de informações jurídicas leva, à hermenêutica jurídica, a necessidade de criação de mecanismos de interpretação sofisticados com elasticidade conceitual e interpretativa, visando abranger situações não previstas pelas normas e captar o real sentido e alcance do texto normativo[85].

Enquadrando-se o caso concreto no conceito abstrato da norma, há a aplicação do direito através da subsunção do fato à norma[86]. No entanto, nem sempre é possível a subsunção, já que a norma não consegue prever e disciplinar todos os acontecimentos que surgem pela dinâmica e complexidade das sociedades humanas.

Nesses casos, busca-se a integração do ordenamento jurídico, visando o preenchimento das lacunas conceituais que possam existir, através da analogia, dos costumes, dos princípios gerais de direito e da equidade.

Para preencher tais lacunas conceituais, lançando-se mão de inúmeros métodos interpretativos, há um grande desafio às habilidades cognitivas dos intérpretes humanos. Tal desafio decorre do grande volume de informações que precisa ser manipulado no processo de interpretação e subsunção da norma ao caso concreto. Para facilitar esse processo interpretativo, a IA pode ser uma grande aliada no sentido de potencializar as habilidades dos intérpretes do direito.

Para entender como funciona a aplicação da *expertise* tecnológica, propiciada pela inteligência artificial, é preciso abordar algumas técnicas da IA utilizadas no âmbito jurídico, como o raciocínio automatizado e a representação do conhecimento.

O raciocínio automatizado tem sido aplicado em sistemas computacionais na área jurídica. Inicialmente, na forma de sistemas especialistas e, mais recentemente, na forma de agentes de *software*[87].

Os sistemas especialistas possuem conhecimento especializado sobre assuntos específicos do Direito e são utilizados para a tomada de processos decisórios e, no âmbito dos

---

[84] GIRARDI, Rosario. Inteligência Artificial Aplicada ao Direito. 1. ed. Edição do autor. Brasil: 2020, p. 39. ISBN 978-65-00-03948-1

[85] GIRARDI, Rosario. Inteligência Artificial Aplicada ao Direito. 1. ed. Edição do autor. Brasil: 2020, p. 39-40. ISBN 978-65-00-03948-1

[86] GIRARDI, Rosario. Inteligência Artificial Aplicada ao Direito. 1. ed. Edição do autor. Brasil: 2020, p. 40. ISBN 978-65-00-03948-1

[87] GIRARDI, Rosario. Inteligência Artificial Aplicada ao Direito. 1. ed. Edição do autor. Brasil: 2020, p. ISBN 978-65-00-03948-1

escritórios de advocacia, para a automatização de tarefas, redução de custos e aumento de lucratividade. Esses sistemas foram criados já nos anos 70 e 80[88].

Esses sistemas, desenvolvidos na área jurídica, foram projetados com base em regras, por meio de inferências dedutivas do tipo "Se premissa (s) então conclusão", e com base em casos, por meio de inferências do raciocínio analógico do tipo "Se problema então solução", representando exemplos ou casos contendo soluções que poderão ser aplicadas em problemas semelhantes[89].

Na área jurídica, podemos citar alguns sistemas especialistas, tais como: o Split-Up, baseado em regras que auxiliam na divisão de bens conjugais em casos de divórcio de acordo com a lei australiana;[90] e o CHIRON, sistema baseado em regras e em casos (sistema híbrido), cuja finalidade é fornecer suporte às decisões de planejamento tributário de acordo com a lei e os códigos tributários dos EUA[91].

A representação do conhecimento, por sua vez, se dá através do processamento semântico, permitindo uma interpretação mais precisa das informações, normas e jurisprudências, favorecendo, assim, a tomada de decisão.

Nesta toada, infere-se que a aplicação das técnicas da IA é ampla e compreende, na prática, sistemas de pesquisa jurídica, estratégia de litígios, serviços jurídicos *online* de autoatendimentos, modelos de resolução de disputas, revisão e análise de contratos, análise de grandes volumes de dados ("big data"), tradução automática etc.

Nos Estados Unidos, por exemplo, a IA tem sido amplamente utilizada no sistema de *Contract Intelligence* – COIN, cuja função é interpretar acordos de empréstimo comercial e analisar acordos financeiros no âmbito dos bancos norte-americanos, sendo o JP Morgan Chase & Co. o maior deles[92].

---

[88] GIRARDI, Rosario. Inteligência Artificial Aplicada ao Direito. 1. ed. Edição do autor. Brasil: 2020, p. 41. ISBN 978-65-00-03948-1

[89] GIRARDI, Rosario. Inteligência Artificial Aplicada ao Direito. 1. ed. Edição do autor. Brasil: 2020, p. 41-42. ISBN 978-65-00-03948-1

[90] GIRARDI, Rosario. Inteligência Artificial Aplicada ao Direito. 1. ed. Edição do autor. Brasil: 2020, p. 42. ISBN 978-65-00-03948-1 apud Zeleznikow, J., Stranieri, A., & Gawler, M. (1995). Project report: Split-Up-A legal expert system wich determines property division upon divorce. Artificial Intelligence and Law, 3 (4), 267-275.

[91] GIRARDI, Rosario. Inteligência Artificial Aplicada ao Direito. 1. ed. Edição do autor. Brasil: 2020, p. 42. ISBN 978-65-00-03948-1apud Sanders, K. E. (1991, May). Representing and reasoning about open-textured predicates. In Proceedings of the 3rd international conference on Artificial intelligence and law, p. 137-144. ACM.

[92] FELIPE, Bruno Farage da Costa; PERROTA, Raquel Pinto Coelho. Inteligência Artificial no Direito: Uma realidade a ser desbravada. Revista de Direito, Governança e Novas Tecnologias, Salvador, v.4, n.1, p. 1-16, jan./jun. 2018.

Com a aplicação dessa tecnologia de COIN, estudos têm demonstrado que o trabalho do advogado é reduzido em 360 mil horas ao ano, além de diminuir o número de equívocos na concessão de serviços de empréstimo ocasionados por erro humano[93].

Nesse mesmo paradigma, podemos citar a tecnologia *Chatbot DoNotPay*, criada e colocada no mercado, em 2016, pelo programador Joshua Browder. O Chatbot é um robô que atua como um "advogado virtual" e atende no Reino Unido e em Nova York[94].

A especialidade do robô, inicialmente, era a realização de contestação de multas por estacionamento em local proibido. Mas, diante do expressivo resultado de sucesso, atualmente a tecnologia tem sido empregada para casos de consumidores insatisfeitos com voos atrasados, na confecção de pedido de asilo de refugiados e no suporte a portadores de HIV que desejam entender melhor os seus direitos.

No Brasil, foi criada, em 2013, na cidade de São Paulo, a empresa Finch Soluções, visando o controle do contencioso de massa do escritório de advocacia JBM & Mandaliti. Pioneiramente, a empresa se destacou pela implementação de robôs de captura de informação, automação e gestão de processos no mundo jurídico e, posteriormente, alargou a sua esfera de atuação para o setor de economia[95].

Outro exemplo, a nível nacional, é a Looplex, plataforma utilizada para automação inteligente de documentos, como petições e contratos. Entre os serviços da inteligência artificial, oferecidos pela plataforma, há a busca por pesquisas jurídicas e a confecção de Smart Contracts[96].

A Legal One é um outro exemplo dessa abordagem. De forma automatizada, a plataforma fornece conteúdo de embasamento para questões jurídicas e realiza a gestão e o controle de processos desde a fase inicial até o encerramento.

---

[93] FELIPE, Bruno Farage da Costa; PERROTA, Raquel Pinto Coelho. Inteligência Artificial no Direito: Uma realidade a ser desbravada. Revista de Direito, Governança e Novas Tecnologias, Salvador, v.4, n.1, p. 1-16, jan./jun. 2018 apud GALEON, Dom.; HOUSER, Kristin. An AI Completed 360,000 Hours of Finance Work in Just Seconds. 2017.

[94] FELIPE, Bruno Farage da Costa; PERROTA, Raquel Pinto Coelho. Inteligência Artificial no Direito: Uma realidade a ser desbravada. Revista de Direito, Governança e Novas Tecnologias, Salvador, v.4, n.1, p. 1-16, jan./jun. 2018.

[95] FELIPE, Bruno Farage da Costa; PERROTA, Raquel Pinto Coelho. Inteligência Artificial no Direito: Uma realidade a ser desbravada. Revista de Direito, Governança e Novas Tecnologias, Salvador, v.4, n.1, p. 1-16, jan./jun. 2018.

[96] FELIPE, Bruno Farage da Costa; PERROTA, Raquel Pinto Coelho. Inteligência Artificial no Direito: Uma realidade a ser desbravada. Revista de Direito, Governança e Novas Tecnologias, Salvador, v.4, n.1, p. 1-16, jan./jun. 2018.

Desta forma, podemos ver como o expressivo avanço da Tecnologia Artificial, tanto a nível nacional quanto internacional, tem demonstrado aumento da produtividade, redução de custos e melhora na qualidade dos serviços prestados.

CONCLUSÃO

O objetivo do presente artigo foi analisar a importância da Inteligência Artificial no mundo jurídico, abordando desde a parte teórica do assunto até a parte empírica de como essa tecnologia pode ser aplicada na prática, sem a pretensão de exaurir este tema tão vasto. A partir disso, chegamos à conclusão de que a IA exerce um papel essencial no desenvolvimento dos trabalhos realizados pelos operadores do Direito.

Em uma realidade caracterizada por um Judiciário congestionado, ou seja, com excesso de demanda, a IA pode ser a solução para dinamizar, efetivar e otimizar os processos decisórios. Isso não significa dizer que o trabalho humano será substituído por operadores autômatos, uma vez que o uso da Inteligência Artificial, nesse contexto, teria por finalidade aumentar a capacidade operativa dos profissionais do Direito, tornando-os capazes de lidar com o excesso de demanda e com o grande volume de informações jurídicas de uma forma mais pragmática, célere e efetiva.

Todavia, apesar dos benefícios que a IA concede ao mundo jurídico, não podemos negar que a falibilidade das ferramentas tecnológicas, bem como a perspectiva influenciadora dos vieses algorítmicos, apresentam riscos ao preceito constitucional do *due process of law*, gênese das garantias constitucionais como igualdade, publicidade, imparcialidade e segurança jurídica, devendo a matéria ser, portanto, regulada com atenção aos princípios da precaução e *accountability*, de modo que possamos gozar de seus benefícios sempre observando e controlando os respectivos riscos.

Ex positis, no âmbito de utilização das IA's, é essencial que os profissionais da área jurídica recorram à ética como instrumento de salvaguarda dos direitos fundamentais, vislumbrando-se a possibilidade de revisão das decisões automatizadas.

REFERÊNCIAS BIBLIOGRÁFICAS

CARNEIRO, Tayná; FALCÃO, Cintia Ramos. **Direito Exponencial: o papel da Novas Tecnologias no Jurídico do Futuro.** 1ª ed. São Paulo: Thomson Reuters Brasil, 2020.

DONEDA, D.C.M.; MENDES, L.S.; SOUZA, C.A.P.; ANDRADE, N.N.G. **Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal.** Pensar: Revista de Ciências Jurídicas, Fortaleza, v.23, n.4, p. 1-17, out./dez.2018.

FEIGELSON, Bruno; MALDONADO, Viviane Nóbrega. **Advocacia 4.0.** 1ª ed. São Paulo: Thomson Reuters Brasil, 2019.

FELIPE, Bruno Farage da Costa; PERROTA, Raquel Pinto Coelho. **Inteligência Artificial no Direito: Uma realidade a ser desbravada.** Revista de Direito, Governança e Novas Tecnologias, Salvador, v.4, n.1, p. 1-16, jan./jun. 2018.

FRAZÃO, Ana; MULHOLLAND, Caitlin. **Inteligência Artificial e Direito: ética, regulação e responsabilidade.** 1ª ed. São Paulo: Thomson Reuters Brasil, 2019.

GABRIEL, Martha. **Você, Eu e os Robôs: Pequeno Manual do Mundo Digital.** 1ª ed. São Paulo: Atlas, 2018.

GIRARDI, Rosario**. Inteligência Artificial Aplicada ao Direito**. 1. ed. Edição do autor. Brasil: 2020, ISBN 978-65-00-03948-1.

MAGRANI, Eduardo. **Entre Dados e Robôs: Ética e Privacidade na Era da Hiperconectividade**. 2ª ed. Porto Alegre: Arquipélago Editorial, 2019.

DE LIMA, Ana Paula M. Canto; HISSA, Carmina Bezerra; SALDANHA, Paloma Mendes. **Direito Digital: Debates Contemporâneos.** 1ª ed. São Paulo: Thomson Reuters Brasil, 2019.

BREVES APONTAMENTOS SOBRE O DIREITO AO ESQUECIMENTO E REDES SOCIAIS

Isabella Macedo Torres[97]

"Eu, agora – que desfecho!
Já nem penso mais em ti...
Mas será que nunca deixo
De lembrar que te esqueci?
Mário Quintana

CONSIDERAÇÕES INICIAIS

A delicadeza contida na contradição do poema de Mário Quintana nos remete à abordagem do direito ao esquecimento na sociedade da informação: a formação do que se denomina memória digital, que compreende o armazenamento de informações em dispositivos tecnológicos, acaba por trazer à tona dados que foram apagados, ou, mais especificamente, que desejam ser esquecidos.

O direito ao esquecimento é tema que não passa ileso a polêmicas: muito embora enxerguemos sua faceta positiva ao ter em mente as lesões aos direitos da personalidade, mantidos sob a égide do princípio da dignidade da pessoa humana, por outro lado, não podemos olvidar da preservação da memória nacional e da construção histórica e axiológica no seio dos indivíduos componentes de uma pátria, além de sua relação intrínseca a um direito fundamental que nos é caro: a liberdade de expressão.

Seu advento se deu antes do surgimento e massificação da internet e da utilização vertiginosa das redes sociais: relacionados à personalidade humana, o direito ao esquecimento é instituto que tem por intuito proteger os indivíduos de divulgação de fatos que não mais desejem que façam parte do imaginário social, tendo por finalidade o resguardo pessoal, além de favorecer a formação e a reconstrução de sua identidade.

É evidente, portanto, que o direito ao esquecimento não está relacionado apenas ao âmbito digital, não obstante nos dias atuais muitas das ações judiciais versem sobre fatos que constam da internet, tendo em vista a substituição dos meios tradicionais de pesquisa e pela cada vez maior utilização das redes sociais.

---

[97] Mestranda em Direito Constitucional pelo PPGDC da Universidade Federal Fluminense – UFF. Pós-graduada em Direito e Advocacia Pública pela Universidade do Estado do Rio de Janeiro – UERJ. Advogada.

Em um mundo cujas fronteiras físicas são distantes, a internet e as redes sociais nos trouxeram uma proximidade outrora impensada: em tempo real, podemos acompanhar o cotidiano de uma pessoa, um evento ou mesmo catástrofes mundiais.

Porém, como se notou anteriormente, os avanços vêm acompanhados de ônus: tamanha exposição, principalmente em tempos de massificação de *fakenews*, tem limite? O direito ao esquecimento, instituto que ainda enfrenta polêmicas, pode ser utilizado no âmbito das redes sociais por indivíduos que se sentirem lesados por alguma exposição indevida ou por um fato que não mais deseje que faça parte de sua história?

O presente artigo tem por escopo tecer breves considerações acerca do direito ao esquecimento, dando-se ênfase à utilização do instituto nas redes sociais, além de trazer à luz algumas questões relacionadas ao limite e ao alcance das decisões referentes ao instituto em âmbito digital.

1. DELINEAMENTO DO DIREITO AO ESQUECIMENTO NO CENÁRIO JURÍDICO

1.1. ASPECTOS GERAIS

Em 2017, a ONG "Artigo 19" publicou em seu sítio eletrônico uma cartilha com subsídios para o processo legislativo relacionado ao direito ao esquecimento, em que se manifestava contra a previsão do instituto como um direito fundamental expresso[98].

Dentre os motivos suscitados, entende que será prejudicial ao direito à privacidade, ao livre fluxo de informações e, consequentemente, ao livre acesso à informação, principalmente a de "utilidade pública sobre governantes ou personalidades de muita projeção". A ONG reconhece que, embora haja legitimidade na desindexação ou remoção de informações em ambiente digital de algumas informações em relação a determinadas pessoas, o acesso à informação pública deve prevalecer no sopesamento de direitos fundamentais, levando-se em consideração a possibilidade de ocultarem-se fatos essenciais à história da nação brasileira[99].

---

[98] "Direito ao esquecimento" no Brasil: subsídios ao debate legislativo. Disponível em https://artigo19.org/centro/wp-content/uploads/2018/09/Direito-ao-Esquecimento-no-Brasil-%E2%80%93-subsidios-ao-debate-legislativo.pdf acesso em 14.01.2021

[99] "Mesmo sabendo que algumas ações que pedem o "direito ao esquecimento" podem ter justificativas legítimas, vale ressaltar o valor, por vezes maior, da informação pública. Episódios históricos ou de alta relevância para a vida social moldam a cultura, a história e a própria vida das pessoas que compartilham tempo e espaço. Eles devem ser protegidos e estar disponíveis ao público", p. 17. "Direito ao esquecimento" no Brasil: subsídios ao debate legislativo. Disponível em https://artigo19.org/centro/wp-content/uploads/2018/09/Direito-ao-Esquecimento-no-Brasil-%E2%80%93-subsidios-ao-debate-legislativo.pdf acesso em 14.01.2021

E essa não foi a única manifestação nesse sentido, pois uma gama de juristas também se manifestou contrariamente ao instituto, respaldando-se, prioritariamente, no direito à preservação da memória e, assim como a ONG, na liberdade de expressão e informação.

Atualmente, porém, tem se reconhecido, tanto na doutrina e na jurisprudência, que, intrinsecamente relacionado aos direitos da personalidade[100], o direito ao esquecimento tem natureza jurídica de direito constitucional implícito, estando relacionado à proteção da vida, honra, imagem e ao nome[101]. E, embora não conste expressamente do rol de direitos fundamentais, foi incluído dentre as tutelas da dignidade da pessoa humana na sociedade da informação, conforme teor do Enunciado 531 da VI Jornada de Direito Civil do Conselho da Justiça Federal[102].

É importante que se destaque que o direito ao esquecimento "não atribui a ninguém o direito de apagar fatos ou de reescrever a História [...]", mas sim "a possibilidade de se discutir o uso que é dado aos fatos pretéritos, mais especificamente o modo e a finalidade com que são lembrados", sendo necessário nos atentarmos ao fato de que o instituto estará sujeito à ponderação quando colidir com demais direitos existentes em nosso ordenamento, analisando-se a situação casuisticamente[103]. Nas palavras de Schreiber:

> "[...] o direito ao esquecimento é, portanto, um direito (a) exercido necessariamente por uma pessoa humana; (b) em face de agentes públicos ou privados que tenham a aptidão fática de promover representações daquela pessoa sobre a esfera pública (opinião social), incluindo veículos de

---

[100] Ingo Sarlet teceu pertinente crítica no sentido do atual "lugar de destaque" que recebeu o direito ao esquecimento, figurando "na atual constelação dos assim chamados 'novos Direitos'", tendo em vista que o instituto precede à sociedade da informação. Salienta, também, que o direito ao esquecimento "não é propriamente uma novidade e muito menos pode ser qualificado como sendo tipicamente um novo direito humano e/ou fundamental". Segundo o autor: "A ideia central que norteia a noção de um direito ao esquecimento diz com a pretensão das pessoas, físicas e mesmo jurídicas, no sentido de que determinadas informações (aqui compreendidas em sentido amplo) que lhes dizem respeito, especialmente àquelas ligadas aos seus direitos de personalidade, ou, no caso das pessoas jurídicas, à sua imagem e bom nome, não sejam mais divulgadas de modo a impedir sejam objeto de acesso por parte de terceiros ou pelo menos que o acesso a tais informações seja dificultado, tudo de modo a propiciar uma espécie de esquecimento no corpo social". SARLET, Ingo Wolfgang. Tema da moda, direito ao esquecimento é anterior à internet. Disponível em https://www.conjur.com.br/2015-mai-22/direitos-fundamentais-tema-moda-direito-esquecimento-anterior-internet acesso em 10.01.2021

[101] SARLET, Ingo Wolfgang. Tema da moda, direito ao esquecimento é anterior à internet. Disponível em https://www.conjur.com.br/2015-mai-22/direitos-fundamentais-tema-moda-direito-esquecimento-anterior-internet acesso em 10.01.2021

[102] Enunciado: A tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento. Justificativa: Os danos provocados pelas novas tecnologias de informação vêm-se acumulando nos dias atuais. O direito ao esquecimento tem sua origem histórica no campo das condenações criminais. Surge como parcela importante do direito do ex-detento à ressocialização. Não atribui a ninguém o direito de apagar fatos ou reescrever a própria história, mas apenas assegura a possibilidade de discutir o uso que é dado aos fatos pretéritos, mais especificamente o modo e a finalidade com que são lembrados.

[103] SCHREIBER, Anderson. **Direitos da personalidade**, pp. 171/172.

> imprensa, emissoras de TV, fornecedores de serviços de busca de internet etc; (c) em oposição a uma recordação opressiva dos fatos, assim entendida a recordação que se caracteriza, a um só tempo, por ser desatual e recair sobre aspecto sensível da personalidade, comprometendo a plena realização da identidade daquela pessoa humana, ao apresentá-la sob falsas luzes à sociedade"[104].

É necessário que se diferencie o que se denomina esquecimento social do esquecimento individual: enquanto aquele se relaciona ao fato de as notícias e eventos terem sua divulgação cessada ao público, este diz respeito à vítima e seus familiares, que têm o direito de que os fatos em questão não tenham mais repercussão social[105].

Não obstante as divergências trazidas à tona e o atual protagonismo no cenário jurídico, o instituto está longe de ser novidade: relacionado ao direito de ex-detentos de dar continuidade às suas vidas sem que estas estivessem relacionadas a crimes cometidos preteritamente[106], o direito ao esquecimento passou a constar na jurisprudência de forma recorrente em nossos tribunais[107], principalmente devido ao vertiginoso crescimento dos meios de comunicação em massa e a exponencial utilização da internet e das redes sociais[108].

---

[104] SCHREIBER, Anderson. **Direito ao esquecimento e proteção de dados pessoais na Lei 13.709/2018**. Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro.

[105] SARLET, Ingo Wolfgang. **Tema da moda, direito ao esquecimento é anterior à internet**. Disponível em https://www.conjur.com.br/2015-mai-22/direitos-fundamentais-tema-moda-direito-esquecimento-anterior-internet acesso em 10.01.2021

[106] Denominado Caso Lebach, o fato ocorreu na Alemanha, durante a década de 70: "Lebach I / 35 BVerfGE 202 (1973): proibiu-se a transmissão em rede de televisão de documentário sobre cidadão preso, às vésperas de ser solto. Considerou-se que a divulgação poderia comprometer a ressocialização do indivíduo e que, em razão do transcurso do tempo, não havia interesse público significativo em divulgar os fatos', havendo, também, o Caso Lebach II, em que "Caso Lebach II / 1 BVerfGE 348/98 (1999): permitiu-se a veiculação de programa de televisão sobre fatos relacionados ao crime cometido por um indivíduo". Supremo Tribunal Federal. **Pesquisa de jurisprudência internacional**. Disponível em <http://www.stf.jus.br/arquivo/cms/jurisprudenciaBoletim/anexo/Pesquisa4ADireitoaoesquecimento.pdf> acesso em 16.01.2021. Dessa forma, devemos nos atentar que o direito ao esquecimento não se refere a instituto vinculado exclusivamente ao âmbito digital.

[107] SCHREIBER, Anderson. **Direitos da personalidade**, p. 170.

[108] Nota Bauman: "Uma vez que finquem seus pés numa escola ou numa comunidade, seja ela física ou eletrônica, os sites de "rede social" se espalham à velocidade de uma "infecção virulenta ao extremo". Com muita rapidez, deixaram de ser apenas uma opção entre muitas para se tornarem o endereço default de um número crescente de jovens, homens e mulheres. Obviamente, os inventores e promotores das redes eletrônicas tocaram uma corda sensível – ou num nervo exposto e tenso que há muito esperava o tipo certo de estímulo. Eles podem ter motivos para se vangloriar de terem satisfeito uma necessidade real, generalizada e urgente. E qual seria ela? "No cerne das redes sociais está o intercâmbio de informações pessoais." Os usuários ficam felizes por "revelarem detalhes íntimos de suas vidas pessoais", "fornecerem informações precisas" e "compartilharem fotografias". Estima-se que 61% dos adolescentes britânicos com idades entre 13 e 17 anos "têm um perfil pessoal num site de rede" que possibilite "relacionar-se on-line". BAUMAN, Zygmunt. **Vida para o consumo, a transformação das pessoas em mercadoria**. Tradução: Carlos Alberto Medeiros. Rio de Janeiro: Jorge Zahar Editor, 2008, p. 6.

O caso que lhe conferiu maior notoriedade foi o julgamento do caso de Mario Costeja Gonzales contra a Google Inc., a Google Spain SL e o jornal *La Vanguardia*. O processo em questão foi instaurado com respaldo da Diretiva 95/46/CE, antiga lei de proteção de dados da União Europeia, que teve vigência até a publicação da atual GDPR – *General Data Protection Regulation*.

Antes de o caso ter sido submetido ao Tribunal Europeu, o autor apresentou pleito perante a Agência Espanhola de Proteção de Dados contra o jornal *La Vanguardia*, *Google Spain SL* e a *Google Inc*., a fim de que fossem omitidos do *google search* resultados referentes a anúncio de venda de imóveis em hasta pública decorrente de um arresto relacionados à recuperação de dívidas com a Seguridade Social. A Agência indeferiu o pedido em relação ao jornal, sob o argumento de que a circulação da notícia se deu a pedido do Ministério do Trabalho, com vistas a atrair um público maior para a hasta, porém, deferiu o pedido em relação à Google.

Por este motivo, a *Google Spain SL* e a *Google Inc.* foram notificadas, mas se opuseram ao pedido, motivo pelo qual a questão foi submetida ao Tribunal Europeu de Direitos Humanos, que considerou que as disposições dos Estados-Membros poderiam ser aplicadas quando o tratamento de dados fosse realizado por empresa que não estivessem localizadas em seu território, mas que destinasse serviços aos cidadãos da União Europeia, fazendo prevalecer as normas de direito internacional.

À época, o Tribunal considerou que o caráter sensível das informações, unido ao tempo transcorrido desde que o fato havia ocorrido, conferia ao autor direito a que os resultados relacionados a fatos que lhe desabonassem fossem suprimidos do *google search*[109].

O caso em comento acabou por conferir ampla notoriedade ao pedido de desindexação e remoção de conteúdo, sobretudo em buscadores de internet, sendo o Brasil um dos protagonistas em pedido de remoção[110].

---

[109] Disponível em http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=PT acesso em 13.01.2021

[110] "Só por uma ferramenta própria, o Google recebeu 3 bilhões de pedidos de remoção de páginas por ofensas de direitos autorais. São 1,4 milhão com solicitação para remoção. Só no último trimestre de 2016, o Google recebeu 15 mil solicitações governamentais para remoções de conteúdo – a maior parte envolvendo assuntos relacionados a segurança nacional, difamação, privacidade, abuso de drogas e nudez. [...]No Brasil, que ocupa o segundo lugar no mundo em termos de solicitações estatais para remoção de conteúdo, foram 1.400 solicitações só no ano passado. Os principais casos dizem respeito a difamação, privacidade e legislação eleitoral". **Direito a esquecimento é mais perigoso que benéfico.**
Disponível em https://www.jota.info/justica/direito-a-esquecimento-e-mais-perigoso-que-benefico-07112017 acesso em 14.01.2021

Especificamente quanto ao Brasil, dois casos trouxeram notoriedade ao direito esquecimento no cenário nacional: um deles se refere à veiculação, pela TV Globo, do extinto programa "Linha Direta", retratando a chacina da Candelária, em que a emissora restou condenada pelo STJ a indenizar um dos réus que, apesar de absolvido, ainda assim teve o nome mencionado no programa; o segundo caso – que, inclusive, está em sede de Recurso Extraordinário (ARE 833248 RG/RJ)[111], tendo o Supremo Tribunal Federal reconhecido a repercussão geral do tema – também se refere à TV Globo contra a família de Ainda Curi, vítima de um crime ocorrido durante a década de 50 no Rio de Janeiro e que teve sua história veiculada pelo mesmo programa[112]. Nesse caso, a família da vítima requereu indenização da emissora alegando constrangimento pela veiculação dos fatos. Inclusive, é interessante notar que o direito ao esquecimento, nesse caso, não foi o fundamento da ação, sendo suscitado apenas em sede de alegações finais.

E é justamente o fato de estar atrelado à dignidade da pessoa humana que a preocupação em relação à (má?) utilização do direito ao esquecimento é recorrente na doutrina: se, por um lado, há o intuito de omitir atos desabonadores da personalidade de um indivíduo ou mesmo o desejo de resguardar fatos pretéritos que não querem ser trazidos à luz; por outro, o instituto pode ensejar a ocultação de acontecimentos caros ao interesse público, e "tem tudo para se transformar no remédio jurídico para políticos, autoridades públicas e poderosos de todo tipo "limparem a sua ficha"[113], apagando registros de episódios pouco edificantes ou impondo mordaças aos críticos e meios de comunicação"[114].

Ao questionar a classificação do direito ao esquecimento como direito fundamental, Daniel Sarmento menciona a jurisprudência do STJ, de acordo com a qual o instituto representa ameaça à pesquisa, estudo e divulgação da História, tendo em vista que "os

---

[111] SUPREMO TRIBUNAL FEDERAL. Acórdão na íntegra disponível em http://portal.stf.jus.br/processos/downloadPeca.asp?id=302238926&ext=.pdf acesso em 16.01.2021

[112] SARLET, Ingo Wolfgang. **Do caso Lebach ao caso Google vs. Agência Espanhola de Proteção de Dados**. Disponível em https://www.conjur.com.br/2015-jun-05/direitos-fundamentais-lebach-google-vs-agencia-espanhola-protecao-dados-mario-gonzalez acesso em 16.01.2021

[113] É o caso, por exemplo, do ex-deputado federal Eduardo Cunha, atualmente preso por denúncias de corrupção, e que propôs Projeto de Lei de apenas um artigo com o intuito de que o direito ao esquecimento fosse positivado em nosso ordenamento jurídico. Disponível em https://www.camara.leg.br/noticias/689545-PROJETO-INSTITUI-DIREITO-AO-ESQUECIMENTO-PENAL-PARA-EX-DETENTOS acesso em 14.01.2021

[114] SARMENTO, Daniel. **Liberdades comunicativas e "direito ao esquecimento na ordem constitucional brasileira**, p. 5. Disponível em Revista Brasileira de Direito Civil – IBDC - ISSN 2358-6974. Volume 7, Jan / Mar 2016. Disponível em file:///C:/Users/isabe/Downloads/76-291-1-PB.pdf acesso em 12.01.2021

direitos fundamentais devem ser assegurados, de forma igual, para todos os que se encontrarem na mesma situação", e tal conclusão advém do princípio da igualdade[115].

Dessa forma, percebe-se a contradição no tocante ao reconhecimento do direito ao esquecimento – cuja própria terminologia é contestada[116] – como direito fundamental, pois colide com a tutela das liberdades de expressão e imprensa, previstas no artigo 5º, IV e IX, e 220 da Constituição da República, que tem posição de preferência "no confronto com direitos da personalidade, como vem reconhecendo o STF e a doutrina"[117].

Embora Sarmento mencione o Superior Tribunal de Justiça, este não é o único entendimento da Corte: o ministro Luis Felipe Salomão, relator do *leadin case* do direito ao esquecimento no Brasil – o Caso Aída Curi –, entende não se tratar de censura, e admite ser possível a remoção de conteúdos que colidam com o instituto do direito ao esquecimento[118].

Por fim, apesar das controvérsias citadas, o direito ao esquecimento, por estar relacionado ao direito de ressocialização do ex-detento, pode ser extraído de alguns dispositivos legais, como é o caso da Lei de Execução Penal brasileira, em seu artigo 202; no Estatuto da Criança e do Adolescente, artigo 143; no Código de Defesa do Consumidor, em seu artigo 43 e no Marco Civil da Internet, nos artigos 3º e 7º (além dos artigos 18 e 19 que tratam sobre a responsabilidade dos provedores, tópico que será abordado posteriormente)[119].

---

[115] SARMENTO, Daniel. **Liberdades comunicativas e "direito ao esquecimento" na ordem constitucional brasileira**, p. 14. Disponível em https://migalhas.uol.com.br/arquivos/2015/2/art20150213-09.pdf acesso em 12.01.2021

[116] Conforme Schreiber: "[...] a expressão direito ao esquecimento talvez não seja a mais exata. Embora consagrada pelo uso doutrinário e jurisprudencial, tal expressão acaba por induzir em erro o intérprete, sugerindo que haveria um direito de fazer esquecer, um direito de apagar os dados do passado ou suprimir referências a acontecimentos pretéritos. Não é disso, todavia, que se trata. O direito ao esquecimento consiste simplesmente de um direito da pessoa humana de se defender contra uma recordação opressiva de fatos pretéritos, que se mostre apta a minar a construção e reconstrução da sua identidade pessoal, apresentando-a à sociedade sob falsas luzes (*sotto falsa luce*), de modo a fornecer ao público uma projeção do ser humano que não corresponde à realidade (atual)". **Direito ao esquecimento e proteção de dados pessoais na Lei 13.709/2018**, p. 374. *In*: Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro.

[117] SARMENTO, Daniel. **Liberdades comunicativas e "direito ao esquecimento" na ordem constitucional brasileira**, p. 19. Disponível em https://migalhas.uol.com.br/arquivos/2015/2/art20150213-09.pdf acesso em 12.01.2021

[118] Coura, Kalleo. TEIXEIRA, Matheus. **Direito ao esquecimento é mais perigoso que benéfico**. Disponível em https://www.jota.info/justica/direito-a-esquecimento-e-mais-perigoso-que-benefico-07112017 acesso em 14.01.2021

[119] CABRERA, Pierina Andrea Aimone. **Direito ao esquecimento na internet: uma comparação entre as legislações do Brasil e Chile**. *In*: Fórum de Cortes Supremas do Mercosul, p. 9. Disponível em http://www.stf.jus.br/repositorio/cms/portalStfInternacional/portalStfCooperacao_pt_br/anexo/Trabalhocorrigido100.pdf acesso em 16.01.2021

1.2. DIREITO AO ESQUECIMENTO E REMOÇÃO DE CONTEÚDO: POLÊMICA ADVINDA DA EXPRESSA PREVISÃO NA GDPR E DA LGPD

Em 2016, foi publicada, no âmbito da União Europeia, a GPDR – *General Data Protection Regulation*, legislação que veio a unificar e regulamentar a proteção de dados, substituindo a então diretiva 95/46/CE. O Brasil, a fim de se adequar às demandas da OCDE – Organização para Cooperação e Desenvolvimento Europeu, publicou a Lei Geral de Proteção de Dados – LGPD, que tem clara influência na legislação europeia.

Em ambos os diplomas consta a previsão da remoção de conteúdo, e, especificamente na GPDR, consta a expressão *right to be forgotten*, que, obviamente, não passou imune a polêmicas doutrinárias.

Não obstante o direito ao esquecimento possua relação à proteção de dados individuais, porém, "as hipóteses de apagamento de dados constantes do regulamento europeu não constituem um mecanismo de tutela da identidade da pessoa em face de recordações opressivas, mas sim remédio associado à dinâmica específica da proteção de dados pessoais"[120].

Dessa forma, o direito ao esquecimento não há que se confundir com o direito ao apagamento ou remoção de dados previstos tanto na GPDR quanto na LGPD, uma vez que aquele instituto se relaciona especificamente com atos ou acontecimentos que desabonem a história de um indivíduo, enquanto o apagamento de dados está relacionado ao tratamento de dados por um operador ou mesmo pedido de remoção pelo titular, conforme mencionam os artigos das legislações em comento, muito embora um pedido baseado no direito ao esquecimento possa guardar relação com o pedido de remoção de dados.

Schreiber, em referência a esclarecimento tecido pela jurista italiana Maria Roana Alegri, esclarece que:

> A qualificação do direito a ser esquecido (Artigo 17), entretanto, é completamente imprópria, uma vez que o GPDR enfatiza a exclusão de dados independentemente de sua circulação pública, sem que o pedido de cancelamento feito pela pessoa a quem os dados se referem seja necessariamente avaliado em relação à liberdade de imprensa dos órgãos de informação [...]. É, portanto, necessário distinguir entre um significado amplo do conceito de direito ao esquecimento como um direito a ser esquecido, que na era da Internet é mais uma aspiração do que uma possibilidade real, e uma abordagem mais restrita, que diz respeito apenas ao perfil do tratamento de dados pessoais, com base nos quais o

[120] SCHREIBER, Anderson. **Direito ao esquecimento e proteção de dados pessoais na Lei 13.709/2018**, pp. 379/380.

> intermediário digital é solicitado a eliminar os que são incorretos, distorcidos ou não são relevantes, o que não garante necessariamente a absoluta indisponibilidade dos dados[121].

Em sentido contrário, porém, recentemente, a Corte Infraconstitucional Alemã, a *Bundesgerichtshof* (BGH), ao se deparar com pedido de remoção de *links* de busca na internet, com base no artigo 17 do GPDR, proferiu o entendimento de que "o direito ao apagamento não se reduz ao simples deletar de dados, mas deve ser entendido normativamente como direito a ser esquecido (*Recht auf Vergessenwerden*), abrangendo o direito a de-listagem (*Auslistungsrecht*) de links dos resultados de busca 'independente da implementação técnica'"[122].

No caso concreto, porém, o pedido foi julgado improcedente tendo o BGH confirmado o entendimento das instâncias inferiores, pois, em colisão com os demais direitos fundamentais, o direito à informação deveria prevalecer – não sendo o direito ao esquecimento, portanto, um direito absoluto. Para que o direito ao esquecimento seja reconheci no caso concreto, é necessário que estejam preenchidos alguns requisitos:

> (a) os dados deixam de ser necessários ao fim que autorizou a coleta ou tratamento; (b) o titular retira o consentimento dado; (c) o titular se opõe ao tratamento e inexistem interesses legítimos prevalentes a justificar o tratamento; (d) os dados pessoais foram tratados ilicitamente; (e) os dados têm de ser apagados para cumprimento de obrigação jurídica e (f) os dados foram colhidos por ocasião de oferta de serviços da sociedade de informação.

Porém, por não ser ilimitado, deve ser feita a ponderação em relação aos demais direitos fundamentais, tendo prevalecido, no caso concreto, o direito à liberdade de expressão.

Percebe-se, dessa forma, que o caso necessita de maior amadurecimento, e apenas casuisticamente poder-se-á estabelecer uma jurisprudência sólida a fim de determinar o teor do artigo 17 do GPDR, entendimento este que certamente terá consequências na jurisprudência e doutrina brasileiras.

2. DIREITO AO ESQUECIMENTO E REDES SOCIAIS: É POSSÍVEL ESQUECER FRENTE À FORMAÇÃO DE UMA MEMÓRIA DIGITAL?

---

[121] SCHREIBER, Anderson. **Direito ao esquecimento e proteção de dados pessoais na Lei 13.709/2018**, pp. 378.
[122] FRITZ, Karina Nunes. **Direito ao esquecimento não é absoluto, diz Bundesgerichtshof**. Disponível em https://migalhas.uol.com.br/coluna/german-report/336206/direito-ao-esquecimento-nao-e-absoluto-diz-bundesgerichtshof acesso em 16.01.2021

Em um mundo globalizado, não se pode negar a importância que as redes sociais desempenham: são fonte não apenas de interação social, mas de comunicação, divulgação de conteúdo e informação[123].

A miríade de dados fornecidos para que se crie um perfil que pode ser personalizado conforme o gosto e as preferências dos usuários torna-os alvo fácil para oferecimento de propagandas e conteúdos suspeitos, com base em algoritmos gerados pela interação em rede: os famosos *likes* e compartilhamentos.

A questão relacionada ao direito ao esquecimento em meio às redes sociais, portanto, se torna mais profunda na medida em que temos a consciência de que vivemos em um ambiente de hiperconectividade, em que é praticamente impossível esquecer algum fato, tendo em vista quatro fatores que delineiam a chamada sociedade da hiperinformação: digitalização, armazenagem barata de informação, recuperação rápida de dados e alcance global da transmissão de informação[124].

Em termos de evolução da internet, vivemos o que hoje se denomina era da *Web* 4.0 ou *Web* predicativa, que passou pelas seguintes etapas:

> Em uma primeira etapa, também chamada *Web* 1.0 (a expressão é de Tim O'Reilly), a *Internet* era tomada, exclusivamente, como um instrumento de busca e obtenção de informações armazenadas em suas redes de dados. A partir de 2004, passou-se a caracterizar a *Internet* pelo termo *Web 2.0*, o que é representado pela ideia de que a rede mundial de computadores permitiu aos usuários ao mais apenas o consumo de informações, mas também a participação na elaboração, construção e gestão do conhecimento disponível na *Internet*. Passamos, assim, a ter a chamada web social ou web colaborativa, a qual originou sítios como *Youtube*, *Wikipedia*, dentre outros. Em terceiro lugar, surge a *Web 3.0*, também denominada de semântica, em que a interação com a realidade se tornou mais precisa, sensível e concreta, graças a uma forma mais aprimorada de definição, ordenação e hierarquização das informações disponíveis [...]. Por fim, identifica-se o surgimento e o processo de maturação (ainda em curso) de uma *Web 4.0* ou *Web* predicativa, a qual, com base em informações disponíveis em seu sistema de dados, consegue antecipar as necessidades dos seus usuários, de

---

[123] "*Most Americans now receive much of their news from social media, and all over the world, Facebook has become central to people's experience of the world. It used to be said that the "Revolution Will Not Be Televised; maybe or maybe not, but you can be pretty sure that the revolution will be tweeted (#Revolution). [...]When people use Facebook to see exactly what they want to see, their understanding of the world can be greatly affected. [...] We are living in different political universes—something like science fiction's parallel worlds. A lot of the supposed news is fake*". SUNSTEIN, Cass R.. **#republic**. *Daily me*, p. 12.

[124] NETO, Arthur Maria Ferreira. **Direito ao esquecimento e sua fundamentação prioritária no livre desenvolvimento da identidade pessoal**, p. 133. Disponível em https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1569/pdf acesso em 15.01.2021

> modo a atuar quase como um centro autônomo de tomada de decisões do particular, como se fosse uma espécie de cérebro paralelo[125].

Portanto, por mais que haja mecanismos que apaguem informações consideradas indesejáveis, o contato com fatos pretéritos acaba por se tornar praticamente inevitável em ambiente virtual, principalmente no que concerne a redes sociais, em que um conteúdo armazenado em algum dispositivo, mesmo estando sob a tutela do direito ao esquecimento, pode novamente vir à tona.

A memória digital acaba por gerar "uma espécie de imortalidade digital", criando "um dever de filtrar, selecionar, ordenar e interpretar um volume estrondoso de informação", o que, em tempos não muito distantes, "a antiga tendência ao esquecimento gradual acabava evitando"[126].

Fatos e notícias veiculadas por redes sociais acabam por ter o mesmo alcance de uma notícia oriunda de uma fonte confiável, havendo, nesse ciclo, riscos maiores, como a disseminação de uma informação falsa[127].

Outra questão que deve ser suscitada é a divulgação por um usuário de rede social, e não por um meio de comunicação oficial, de fatos que queiram ser "esquecidos" por alguém. Haverá responsabilidade do usuário pela divulgação, caso esteja ciente da proibição e das consequências de seus atos, mas questiona-se se isso não se configuraria em ato de censura por parte do poder público, que acaba por selecionar o que pode ou não ser divulgado. E mais: caso essa informação seja compartilhada em uma ou mais redes sociais por outros usuários, a quem caberá a responsabilização para além das plataformas digitais?

Sendo assim, estará em jogo a ponderação entre o direito à liberdade de expressão e/ou informação e o direito ao esquecimento, com respaldo no direito à privacidade – e, no caso das redes sociais, em que uma informação ou conteúdo pode ser compartilhado infinitas vezes e ter seu alcance, inclusive, perdido de vista, a questão se torna um pouco mais complexa.

---

[125] NETO, Arthur Maria Ferreira. **Direito ao esquecimento e sua fundamentação prioritária no livre desenvolvimento da identidade pessoal**, p. 129, disponível em https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1569/pdf acesso em 15.01.2021

[126] NETO, Arthur Maria Ferreira. **Direito ao esquecimento e sua fundamentação prioritária no livre desenvolvimento da identidade pessoal**, pp 133/134, Disponível em https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1569/pdf acesso em 15.01.2021

[127] SUNSTEIN, Cass R., p. 133.

É importante que nos atentemos, também, nesse caso, à nova concepção que se emprega ao direito à privacidade, que inicialmente relacionava-se a uma conduta absenteísta do Estado quanto à esfera individual, e, com a evolução tecnológica, passou a se tornar ainda mais complexo, tendo em vista que o indivíduo tem direito à privacidade dos dados que circulam no cenário público, sobretudo em rede. Trata-se de conceito que salienta a importância do consentimento do titular dos dados em um contexto de autodeterminação informativa, e lhe confere a ciência sobre a "movimentação" de suas informações[128] – muito embora, na prática, a autodeterminação informativa acabe por se constituir em uma falácia, conforme se esclareceu anteriormente.

Há entendimentos no sentido de que a autodeterminação informativa "transmite com clareza a noção de que o direito ao esquecimento se relaciona mais diretamente com o direito à identidade do que com o direito à privacidade, mesmo que com esse mantenha conexão relevante"[129].

Com um clique, pode-se colocar em risco a vida e reputação de uma pessoa, pois quem compartilha conta com a certeza da impunidade devido à "aparência de anonimato e a facilidade de abusos", sobretudo em se tratando de redes sociais, em que existe a possibilidade já abordada de criação de perfis falsos[130].

Os artigos 18 e 19 do Marco Civil da Internet estabelecem que a responsabilidade por conteúdo gerado por terceiros será destes, e não dos provedores de internet. O artigo 19, especificamente, prevê que "uma plataforma só pode ser responsabilizada civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para removê-lo".

O referido artigo, entretanto, tem sua constitucionalidade questionada, e é alvo de dois Recursos Especiais com repercussão geral que serão em breve analisados pelo Supremo Tribunal Federal: o primeiro deles é o RE 1057258, oriundo do estado de Minas Gerais, em que se requereu a remoção de uma página da extinta comunidade Orkut, de propriedade da Google, denominada "Eu odeio a Aliandra", o segundo, RE 1037396, se refere a decisão que

---

[128] RODOTÁ, Stephano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodan de Moraes. Tradução: Danilo Doneda. Rio de Janeiro: Renovar, 2008, p. 16

[129] PP. 143/144. Disponível em https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1569/pdf acesso em 16.01.2021

[130] LEONARDI, Marcel, p. 357.

determinou a exclusão de um perfil falso no Facebook, tendo o processo tramitado em São Paulo[131].

O direito ao esquecimento, portanto, tem novos contornos na era da hiperconectividade, quando os avanços tecnológicos são considerados, pois é evidente que "criam inéditos conflitos envolvendo o manejo, a transmissão e a guarda de dados pessoais por parte de órgãos governamentais e de entidades privadas, o que acaba impondo uma reconfiguração nos espaços público e privado"[132].

Além disso, o debate sobre o direito ao esquecimento também se direciona para questões de direito processual. Nesta seara, visando a evitar restrições à liberdade de expressão e informação de forma generalizada e global, a doutrina estrangeira tem se valido do *scope of jurisdiction* ou eficácia territorial da jurisdição – esclarecendo-se que escopo é utilizado no sentido de amplitude da decisão, e não objetivo[133] –, que tem por intuito limitar o alcance de decisões judiciais relacionadas à internet, restringindo a eficácia do julgado que determinar a remoção de uma postagem apenas ao território de onde adveio[134].

É o caso, por exemplo, que recentemente ocorreu na França, envolvendo pedido de desindexação de resultados de pesquisa feito agência francesa de proteção de dados, CNIL – *Comission Nationale de l'Informatique et des Libertés*, contra a Google: para a CNIL, a ordem judicial deveria ser aplicada a todo o domínio de seus resultados de busca (google.com). A empresa recorreu ao Tribunal Administrativo Francês, *Conseil d'État*, que submeteu a questão ao Tribunal de Justiça da União Europeia[135], que, mesmo reafirmando o entendimento de que os titulares de dados têm o direito a serem esquecidos quando houver violação do

---

[131] OYAMA, Érico. **Direito ao esquecimento pode ganhar força se o STF derrubar artigo 19 do Marco Civil**. Disponível em https://www.jota.info/coberturas-especiais/liberdade-de-expressao/direito-ao-esquecimento-marco-civil-24012020#:~:text=Esse%20artigo%20define%20que%20uma,express%C3%A3o%20e%20impedir%20a%20censura. Acesso em 14.01.2021

[132] NETO, Arthur Maria Ferreira. **Direito ao esquecimento e sua fundamentação prioritária no livre desenvolvimento da identidade pessoal**, p. 145. Disponível em https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1569/pdf acesso em 15.01.2021

[133] LAUX, Francisco de Mesquita. **Redes sociais e limites da jurisdição: análise sob a ótica da territorialidade e da efetividade com o auxílio da tecnologia**. *In*: Inteligência artificial e direito processual, p. 568.

[134] LAUX, Francisco de Mesquita. **Redes sociais e limites da jurisdição: análise sob a ótica da territorialidade e da efetividade com o auxílio da tecnologia**. *In*: Inteligência artificial e direito processual, p. 559.

[135] HENRIQUES, Mariana Mello. **Corte Europeia impõe limites do direito ao esquecimento**. Disponível em http://gcalaw.com.br/corte-europeia-impoe-limites-do-direito-ao-esquecimento/ acesso em 13.01.2021

regulamento ou o direito da União ou dos Estados-membros que se apliquem ao responsável pelo tratamento, restringiu o alcance da decisão ao território da União Europeia[136].

Quanto aos tribunais pátrios, não há um claro posicionamento a ser aplicado – uma preocupação que deve estar presente na ordem do dia, uma vez a maior importância conferida aos precedentes com o advento do Código de Processo Civil de 2015. Inclusive, Ingo Sarlet, ao se referir ao direito ao esquecimento na jurisprudência pátria, tece importante crítica em relação a ser ou não um direito autônomo e a definição de seu âmbito de incidência, não deixando de notar a relevância dessa determinação, uma vez que "implica importantes consequências [...] no trato do objeto das posições subjetivas correlatas e dos respectivos deveres de proteção estatais, assim como no caso do controle judicial da legitimidade constitucional das restrições"[137].

Conforme nota Francisco Laux, não há julgamento colegiado nos Tribunais Superiores brasileiros que empregue esse critério, existindo, porém, algumas decisões monocráticas do Ministro Alexandre de Moraes de julho de 2020, no Inquérito 4781/DF, em que se determinou o bloqueio de perfis do Facebook e do Twitter, tendo, contudo, o Facebook se negado a cumprir a determinação. Por sua vez, o Tribunal de Justiça de São Paulo indeferiu pedidos de ampliação direta de extensão territorial em algumas oportunidades – como ocorreu, por exemplo, em 2016, em que apreciou demanda de remoção de postagens no Twitter e, em outra oportunidade, bloqueio de acesso a vídeos no Youtube, e, em ambas as oportunides, restringiu-se o alcance da decisão ao âmbito local[138].

Deve-se notar, porém, que qualquer conteúdo postado em uma rede social está sujeito ao fenômeno da viralização e que, portanto, a remoção de perfis acaba por não ser efetiva, uma vez que: "(i) outros podem continuar disseminando a mesma informação e (ii) porque os próprios usuários atingidos pela determinação podem criar outras contas e manter a divulgação de informações já tidas como ofensivas pelos tribunais"[139].

---

[136] VALENTE, Fernanda. **Direito ao esquecimento deve ser aplicado em toda a União Europeia, decide tribunal**. Disponível em https://www.conjur.com.br/2019-set-24/direito-esquecimento-aplicado-toda-uniao-europeia acesso em 13.01.2021

[137] SARLET, Ingo Wolfgang. **Vale a pena relembrar o que estamos fazendo com o direito ao esquecimento**. Disponível em https://www.conjur.com.br/2018-jan-26/direitos-fundamentais-vale-pena-relembrar-fizemos-direito-esquecimento acesso em 10.01.2021

[138] LAUX, Francisco de Mesquita, pp. 570-572.

[139] LAUX, Francisco de Mesquita, p. 576.

O presidente do ITS – Instituto de Tecnologia e Sociedade, Carlos Affonso de Souza, ao discorrer sobre a questão do escopo da jurisdição, se refere ao caso francês, e esclarece que, apesar de ter representado uma vitória ao Google, o acompanhamento da medida de acesso aos links removidos demandará medidas dos países membros da União Europeia. Apesar disso, devemos nos atentar ao perigo da remoção global de links, principalmente pelo fato de que acaba por se nivelar por baixo o direito à liberdade de expressão. O jurista ilustra com o exemplo da Tailândia, país em que comentários negativos sobre a autoridade real é considerado crime: caso nesse país haja uma determinação em escala global, demais países, cujo alcance da liberdade de expressão é mais amplo, seriam afetados diretamente[140].

Os tribunais brasileiros, como se referenciou anteriormente, tem seguido essa linha de raciocínio, mas não deixa de ser motivo para acompanhar as decisões, tendo em vista as polêmicas que existem em relação ao direito ao esquecimento.

Para além da intervenção do judiciário, analisando-se a questão sob a ótica administrativa, não se pode deixar que o ambiente virtual também está sujeito a normas de regulação, principalmente no que concerne a práticas como a autorregulação regulada, que tem se mostrado recorrentes em plataformas das redes sociais. A autorregulação regulada concilia características da autorregulação e da heterorregulação, e, a partir dessa perspectiva, a iniciativa privada, através da própria plataforma da rede social, aplica suas regras específicas, enquanto o Estado, cujos conhecimentos não são tão sofisticados, emprega técnicas de coerção, para que prevaleça o interesse público[141].

Este é o caso do Facebook, que conta com o *overboardsight*[142], espécie de comitê de supervisão que tem o intuito de auxiliar a plataforma em questões envolvendo remoção de conteúdo. Conforme informações constantes no sítio eletrônico do Comitê de Supervisão, suas decisões terão caráter vinculante, devendo, portanto, ser implementadas pelo Facebook, a não ser que configurem violação legal[143].

---

[140] SOUZA, Carlos Affonso de. **Ao limitar direito ao esquecimento do Google, Europa cria outros problemas**. Disponível em https://tecfront.blogosfera.uol.com.br/2019/09/25/europa-limita-direito-ao-esquecimento-do-google-mas-mexe-nas-buscas/ acesso em 14.01.2021

[141] LAUX, Francisco de Mesquita, p. 581.

[142] https://oversightboard.com/

[143] Overboard Sight. Comitê de Supervisão. Garantir o respeito à liberdade de expressão por meio do julgamento independente. Disponível em https://oversightboard.com/ acesso em 16.01.2021

Nesse caso, ocorre uma ação híbrida: remoção manual e mediante mecanismos de inteligência artificial, baseadas em denúncias dos usuários. Tais atos têm se aplicado, principalmente, quanto a *hate speech*[144], porém, nada impede que essas ferramentas sejam também utilizadas a denúncias quanto a conteúdos que estejam sob a tutela do direito ao esquecimento, quando este for reconhecido pelo Estado.

Inclusive, há normas em alguns países que contam com a ação individual junto à rede social antes que a pessoa acione o judiciário, como no Direito Espanhol, em que há normativas que reconhecem que, para que seja exercido o direito ao esquecimento, é necessário que o indivíduo siga alguns passos, sendo o primeiro deles requerer, junto à rede social, a remoção do conteúdo mediante o preenchimento de formulários disponibilizados aos usuários. Caso não haja resposta, poderá entrar em contato com a autoridade de proteção de dados, e, se ainda assim não houver solução, poderá acionar a justiça para a remoção com respaldo no direito ao esquecimento[145].

Na Alemanha, por sua vez, conforme estudos do professor Ricardo Campos na *Goethe Universität Frankfurt*, apontam que "aquele país tem se aproximado cada vez mais de uma responsabilidade do meio", devendo a plataforma se tornar responsável quando não promover "procedimentos para notificação, remoção de conteúdo e direito de defesa", de acordo com o *Network Enforcement Act* (NetzDG), lei de 2017 que "exige que determinadas plataformas mantenham procedimentos efetivos para processar reclamações sobre conteúdo ilegal"[146].

Porém, embora a princípio pareça simples e imediata a resposta da regulatória – especificamente a conjunta, conforme se mencionou acima –, há quem não a veja com bons olhos, respondendo de forma negativa a qualquer interferência governamental em ambiente digital, e defendendo que o ambiente virtual deveria ser uma *free zone*. Na década de 90, o ativista John Perry Barlow elaborou a *Declaration of the independence of cyberspace*, argumentando que o governo não possui qualquer soberania no que tange à regulação da

---

[144] LAUX, Francisco de Mesquita, pp. 582/583.

[145] QUESADA, Francisco Mesa. **Dimensión constitucional del derecho al olvido**, p. 25. Disponível em https://www.derechoycambiosocial.com/revista049/DIMENSION_CONSTITUCIONAL_DEL_DERECHO_AL_OLVIDO.pdf acesso em 13.01.2021

[146] VAINZOF, Rony. **Desinformação, autorregulação regulada e responsabilidade das plataformas**: quem deve atuar na linha de frente contra a desinformação, o Judiciário ou as plataformas? Disponível em https://www.jota.info/opiniao-e-analise/artigos/desinformacao-autorregulacao-regulada-e-responsabilidade-das-plataformas-17072020 acesso em 16.01.2021

internet[147], ideia esta que ainda continua em voga, como podemos observar frequentemente nos noticiários.

Cass Sustein sustenta que qualquer oposição veemente contra a regulação por parte do ente governamental é incoerente, tendo em vista que cotidianamente estamos expostos a ataques à privacidade e até mesmo ameaças em relação a arquivos de interesse da segurança nacional. O problema, segundo o autor, não deve dizer respeito à regulação em si, mas ao tipo de regulação que será executada. Nota, ainda, que não apenas os cidadãos têm benefícios advindos de um ambiente regulado, mas também os prestadores de serviço – e, nesse caso específico, os provedores de serviço de internet e redes sociais:

> *If you have a Facebook account, you didn't pay for it. But it's definitely yours. If someone commandeers your account and starts posting pictures of Stalin with accompanying text ("the greatest person who ever lived!"), your rights have been violated. You can probably get legal recourse. The same thing is true of your Twitter account. If someone sends out tweets under your name ("qcfgvwav" or "Twitter is Satan's toolbox"), they have intruded on what is, in a legal sense, your property. For both Facebook and Twitter, that's important.*
>
> *Though many people don't think of them this way, property rights, when conferred by law, are a quintessential form of government regulation. They create and limit power. They determine who owns what, and they say who may do what to whom. They allow some people to exclude others. That's regulation, in a nutshell*[148].

O autor enfatiza, porém, que a existência de um ambiente virtual regulado não significa que esta deverá ser feita de forma ostensiva, mas efetiva, reforçando, portanto, a questão, que deve ser direcionada não à existência de regulação em ambiente virtual, mas à forma como ela deve ser feita: quando o governo cria e protege direitos, e quando proíbe as pessoas de agirem conforme suas próprias vontades, independentemente da vontade alheia, o governo está exercendo regulação. Portanto, a internet está longe de ser um espaço onde não há vigência de lei ou isenta de regulação[149].

---

[147] SUNSTEIN, Cass R., p. 164. Nota o autor que: "*Perhaps the argument is rooted in something else: a general hostility to any form of government regulation. This is, of course, a pervasive kind of hostility. A common argument is that legal interference with the communications market should be rejected simply because it is a form of government regulation, and be disfavored for exactly that reason. It is certainly easy to find that claim on Facebook and Twitter".*

[148] *SUNSTEIN, Cass R., pp. 164*/165.

[149] SUNSTEIN, Cass R., pp. 176/177.

A verdade é que novamente nos deparamos com a colisão de direitos fundamentais: se, por um lado, a sociedade tem direito à informação e à memória, conforme anteriormente se pontuou, por outro, a pessoa tem direito a resguardar sua vida privada e intimidade.

As ações das agências de proteção de dados europeias, embora se mostrem eficientes – como se notou em ambos os casos discutidos anteriormente –, exige que haja atitudes conjuntas com as empresas privadas, pois apenas a ação do judiciário não é suficiente para que os direitos da personalidade sejam respeitados em rede, devido ao alcance desproporcional e a velocidade com que se propaga a informação.

Quanto às sentenças, principalmente no tocante ao direito ao esquecimento, a preocupação de muitos juristas é a de que não apenas as redes sociais, que contam com filtros e mecanismos de denúncia para a remoção de determinado conteúdo cujo acesso tenha sido proibido pelo tribunal sob o prisma do direito ao esquecimento, mas a de que as plataformas acabem se tornando censores prévios quanto ao conteúdo que pode ou não ser visualizado em redes e demais mecanismos de pesquisa[150].

É por esse motivo que o direito ao esquecimento, conquanto defendido por um lado, conta com ferrenhas oposições, tendo em vista a primordial importância do direito à liberdade de informação, e um sopesamento judicial nos remete à ponderação.

CONCLUSÕES

Conforme se contata, apesar de não constituir um direito positivado, ao direito ao esquecimento foi conferida natureza jurídica de direito constitucional implícito, e, apesar da frequência com que está presente no cotidiano dos Tribunais, ainda enfrenta polêmicas e divergências, principalmente quando se considera a importância da formação à memória e o direito à liberdade de expressão – valores caros, ainda mais considerando-se o contexto de fragilidade democrática que enfrentam países como o Brasil.

No âmbito das redes sociais, o tema se torna um pouco mais complexo, sobretudo na era da hiperconectividade, em que forma-se, com facilidade, uma memória digital, cujo

[150] É como se sustenta a jurisprudência do Superior Tribunal de Justiça, em que há precedentes nesse sentido, tal qual se extrai do seguinte trecho: “A jurisprudência desta Corte Superior tem entendimento reiterado no sentido de afastar a responsabilidade de buscadores da internet pelos resultados de busca apresentados, reconhecendo a impossibilidade de lhe atribuir a função de censor e impondo ao prejudicado o direcionamento de sua pretensão contra os provedores de conteúdo, responsáveis pela disponibilização do conteúdo indevido na internet”. REsp RECURSO ESPECIAL Nº 1.660.168 - RJ (2014/0291777-1).

conteúdo pode vir à tona independentemente da vontade do sujeito que deseja esquecer. Consequentemente, a autodeterminação informativa, considerada essencial a fim de que os indivíduos tenham ciência quanto ao destino de seus dados, acaba por ser considerada uma falácia, por mais que um fato esteja sob a tutela do direito ao esquecimento.

Atualmente, no cenário jurídico, analisar-se-ão a constitucionalidade do artigo 19 do Marco Civil da Internet, que isenta as plataformas de responsabilidade por conteúdos postados por terceiros – aplicando-se esse caso aos usuários de redes sociais – bem como o ARE Recurso Extraordinário (ARE 833248 RG/RJ), referente ao caso Aída Curi, em que se discute o reconhecimento do direito ao esquecimento.

Ambos os julgamentos serão determinantes no que concerne à responsabilidade por conteúdos que estejam sob a tutela do direito ao esquecimento em âmbito digital, ainda mais se considerarmos que um conteúdo compartilhado pode acabar sendo perdido de vista.

Deve-se ressaltar, também, o delineamento quanto ao alcance das decisões jurisdicionais: a jurisprudência pátria, com respaldo na doutrina estrangeira, tem aplicado o *scope of jurisdiction*, restringindo o alcance da decisão emanada ao âmbito do território de onde adveio, fato este que se torna relevante, principalmente quando temas como a liberdade de expressão tem diferentes abordagens dependendo de onde esteja sendo analisada.

Outro recurso que vem sendo aplicado é a autorregulação regulada, que consiste na ação híbrida de agentes da iniciativa privada e o poder público, que, atuando em conjunto, muitas vezes até mesmo contando com denúncias e ações individuais, pode determinar o que será ou não removido das redes sociais. É o caso, por exemplo, do *overboardsight*, comitê que atua em conjunto com o Facebook, e que tem decisões de caráter vinculante.

O tema, portanto, está longe de ser pacífico e há, ainda, um longo caminho a ser percorrido, ainda mais quando também nos deparamos com polêmicas advindas da interpretação conferida aos regulamentos de proteção de dados recentemente publicados.

Enquanto isso, continuaremos na difícil tarefa de esquecer, pois mesmo que um conteúdo seja excluído, é com a memória humana que temos de lidar, no final das contas.

REFERÊNCIAS

Artigo 19. “Direito ao esquecimento” no Brasil: subsídios ao debate legislativo. Disponível em https://artigo19.org/centro/wp-content/uploads/2018/09/Direito-ao-Esquecimento-no-Brasil-%E2%80%93-subsidios-ao-debate-legislativo.pdf acesso em 14.01.2021

BAUMAN, Zygmunt. *Vida para o consumo, a transformação das pessoas em mercadoria*. Tradução: Carlos Alberto Medeiros. Rio de Janeiro: Jorge Zahar Editor, 2008.

InfoCuria Jurisprudência. Disponível em http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=PT acesso em 13.01.2021

CABRERA, Pierina Andrea Aimone. **Direito ao esquecimento na internet: uma comparação entre as legislações do Brasil e Chile**. *In*: Fórum de Cortes Supremas do Mercosul. Disponível em http://www.stf.jus.br/repositorio/cms/portalStfInternacional/portalStfCooperacao_pt_br/anexo/Trabalhocorrigido100.pdf acesso em 16.01.2021 acesso em 16.01.2021

CARRILLO, Marc. **El derecho al olvido em internet**. Disponível em https://elpais.com/diario/2009/10/23/opinion/1256248805_850215.html acesso em 13.01.2021

Coura, Kalleo. TEIXEIRA, Matheus. **Direito ao esquecimento é mais perigoso que benéfico**. Disponível em https://www.jota.info/justica/direito-a-esquecimento-e-mais-perigoso-que-benefico-07112017 acesso em 14.01.2021

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

FRITZ, Karina Nunes. **Direito ao esquecimento não é absoluto, diz Bundesgerichtshof**. Disponível em https://migalhas.uol.com.br/coluna/german-report/336206/direito-ao-esquecimento-nao-e-absoluto-diz-bundesgerichtshof acesso em 16.01.2021

HENRIQUES, Mariana Mello. **Corte Europeia impõe limites do direito ao esquecimento**. Disponível em http://gcalaw.com.br/corte-europeia-impoe-limites-do-direito-ao-esquecimento/ acesso em 13.01.2021

LAUX, Francisco de Mesquita. **Redes sociais e limites da jurisdição: análise sob a ótica da territorialidade e da efetividade com o auxílio da tecnologia**. *In*: Inteligência artificial e direito processual.

LEONARDI, Marcel.

NETO, Arthur Maria Ferreira. **Direito ao esquecimento e sua fundamentação prioritária no livre desenvolvimento da identidade pessoal**. Disponível em https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1569/pdf acesso em 15.01.2021

OYAMA, Érico. **Direito ao esquecimento pode ganhar força se o STF derrubar artigo 19 do Marco Civil**. Disponível em https://www.jota.info/coberturas-especiais/liberdade-de-expressao/direito-ao-esquecimento-marco-civil-

24012020#:~:text=Esse%20artigo%20define%20que%20uma,express%C3%A3o%20e%20impedir%20a%20censura acesso em 15.01.2021

QUESADA, Francisco Mesa. **Dimensión constitucional del derecho al olvido**, p. 8. Disponível em https://www.derechoycambiosocial.com/revista049/DIMENSION_CONSTITUCIONAL_DEL_DERECHO_AL_OLVIDO.pdf acesso em 13.01.2021

RODOTÁ, Stephano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodan de Moraes. Tradução: Danilo Doneda. Rio de Janeiro: Renovar, 2008.

SCHREIBER, Anderson. **Direitos da personalidade**.

_____**Direito ao esquecimento e proteção de dados pessoais na Lei 13.709/2018**. Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro.

SARLET, Ingo Wolfgang. **Do caso Lebach ao caso Google vs. Agencia Espanhola de Proteção de Dados**. Disponível em https://www.conjur.com.br/2015-jun-05/direitos-fundamentais-lebach-google-vs-agencia-espanhola-protecao-dados-mario-gonzalez acesso em 16.01.2021

_____**Tema da moda, direito ao esquecimento é anterior à internet**. Disponível em https://www.conjur.com.br/2015-mai-22/direitos-fundamentais-tema-moda-direito-esquecimento-anterior-internet acesso em 10.01.2021

_____**Vale a pena relembrar o que estamos fazendo com o direito ao esquecimento**. Disponível em https://www.conjur.com.br/2018-jan-26/direitos-fundamentais-vale-pena-relembrar-fizemos-direito-esquecimento acesso em 10.01.2021

SARMENTO, Daniel. **Liberdades comunicativas e "direito ao esquecimento" na ordem constitucional brasileira**, p. 5. Disponível em Revista Brasileira de Direito Civil – IBDC - ISSN 2358-6974 Volume 7 Jan / Mar 2016
file:///C:/Users/isabe/Downloads/76-291-1-PB.pdf

SOUZA, Carlos Affonso. **Ao limitar direito ao esquecimento do Google, Europa cria outros problemas**.
Disponível em https://tecfront.blogosfera.uol.com.br/2019/09/25/europa-limita-direito-ao-esquecimento-do-google-mas-mexe-nas-buscas/ acesso em 14.01.2021

SUNSTEIN, Cass R.. **#republic**: divided democracy in the age of social media.

VAINZOF, Rony. **Desinformação, autorregulação regulada e responsabilidade das plataformas**: quem deve atuar na linha de frente contra a desinformação, o Judiciário ou as plataformas? Disponível em https://www.jota.info/opiniao-e-analise/artigos/desinformacao-autorregulacao-regulada-e-responsabilidade-das-plataformas-17072020 acesso em 16.01.2021

VALENTE, Fernanda. **Direito ao esquecimento deve ser aplicado em toda a União Europeia, decide tribunal**. Disponível em https://www.conjur.com.br/2019-set-24/direito-esquecimento-aplicado-toda-uniao-europeia acesso em 13.01.2021

http://www.stf.jus.br/arquivo/cms/jurisprudenciaBoletim/anexo/Pesquisa4ADireitoaoesquecimento.pdf

A TECNOLOGIA DE DADOS NA INDÚSTRIA DO PETRÓLEO 4.0

Wagner da Silva Reis

1. INTRODUÇÃO

O tema mais amplo do presente texto é a Indústria do Petróleo 4.0, sua característica disruptiva, o cenário que se descortina nos próximos meses. Não seria possível em sede de um opúsculo enfrentar todos os aspectos que essa "virada de Copérnico" representa para a indústria de petróleo e gás. Mas, tem-se aqui a pretensão de abordar tecnologias de dados que já promovem mudanças significativas, e desafiam a regulação estatal, o direito dos contratos, o direito econômico e outros ramos. São tecnologias que afetam o mundo todo, e que já vem sendo implementadas há pelo menos uma década. O objetivo é apresentar o impacto das tecnologias de Big Data e Blockchain na Indústria do Petróleo 4.0. Nesse sentido, numa primeira fase, apresentar-se-á a indústria do petróleo e seus segmentos, para de forma propedêutica, iniciar o leitor nas suas especificidades; numa outra fase será enfrentada a tecnologia de Big Data e os aspectos de cibersegurança envolvidos na aplicação da mesma na Indústria de Petróleo e Gás 4.0; a seguir o texto avança para a apresentação da tecnologia Blockchain na Indústria de Petróleo e Gás 4.0 e suas relações com a internet das coisas Indústrial; e finalmente, será abordado o papel da tecnologia na prevenção de fraudes marítimas no segmento downstream da Indústria de Petróleo e Gás 4.0. Esse percurso iniciar-se-á após a presente introdução e se encerrará com uma conclusão que pretende atingir o objetivo acima proposto.

2. A INDÚSTRIA DO PETRÓLEO

Em apertada síntese, a expressão "indústria do petróleo"[151] envolve toda uma gama de esforços no sentido de explorar e produzir petróleo. Nesse sentido, adotaremos aqui três segmentos dessa indústria: upstream, midstream e downstream. Por upstream entende-se o início da cadeia logística, que antecede ao beneficiamento, compreende a pesquisa ou exploração[152]; lavra ou produção[153]; desenvolvimento[154]. Vale ressaltar que o transporte será incluído neste segmento se o fizer com o produto em estado natural. A expressão midstream possui a ideia das atividades de captação do que é proveniente do upstream, beneficiamento, e transporte. E downstream é entendido como o segmento da

151 conjunto de atividades econômicas relacionadas com a exploração, desenvolvimento, produção, refino, processamento, transporte, importação e exportação de petróleo, gás natural e outros hidrocarbonetos fluidos e seus derivados. (Lei nº 9.478/1997, Art. 6, inciso XIX)

152 conjunto de operações ou atividades destinadas a avaliar áreas, objetivando a descoberta e a identificação de jazidas de petróleo ou gás natural (Lei nº 9.478/1997, Art. 6, inciso XV)

153 conjunto de operações coordenadas de extração de petróleo ou gás natural de uma jazida e de preparo para sua movimentação. (Lei nº 9.478/1997, Art. 6, inciso XVI)

154 conjunto de operações e investimentos destinados a viabilizar as atividades de produção de um campo de petróleo ou gás. (Lei nº 9.478/1997, Art. 6, inciso XVII)

distribuição e comercialização dos derivados de petróleo e gás. Interessante pontuar que há quem suprima o midstream, redistribuindo atividades entre os outros segmentos. (QUINTANS, 2015, pp.70 a 74)

Segundo a empresa KPMG:

> A dinâmica do setor de Petróleo e Gás desafia as empresas a buscarem uma atualização contínua sobre uma série de temas como regulações, pesquisa e desenvolvimento, meio ambiente, legislação e logística para que consigam mitigar riscos que comprometam a continuidade e a competitividade do negócio. A KPMG tem hoje estruturada uma das maiores práticas de Petróleo e Gás do País com profissionais de Audit, Tax e Advisory focados em empresas do setor, que atuam tanto na atividade exploratória quanto na cadeia de suprimentos, e que podem lhe ajudar a lidar com os desafios do mercado, gerando valor hoje que permita o planejamento do amanhã. (KPMG, 2020)

A ANP iniciou em outubro de 2020 uma consulta pública, a qual se seguirá uma audiência pública em dezembro[155], sobre a minuta de resolução que visa regulamentar o exercício da atividade de produção de derivados de petróleo e gás natural.

O que se denominou como Indústria 1.0 foi uma fase da Indústrialização na qual as máquinas a vapor passaram a potencializar a produção por intermédio da mecanização no século XIX. Uma das consequências destas mudanças foi a necessidade de descentralização da tomada de decisão.

Em um outro momento, já com o termo Indústria 2.0, a mudança se deu pelo uso da energia elétrica em substituição ao vapor, o que conferiu mais eficiência aos sistemas; ocorrendo nesta fase a implantação da linha de montagem e a produção em larga escala.

Por volta da década de 1970 iniciou-se a chamada Indústria 3.0 onde as máquinas passaram a ter integrados sistemas computacionais, e esta fase foi caracterizada pela automação, e a intervenção humana foi paulatinamente sendo substituída por robôs.

O conceito de Indústria 4.0 considera paradigmas e tecnologias disruptivas, inovam radicalmente em relação às práticas desenvolvidas anteriormente, e isso ocorre pelo desenvolvimento colaborativo de produtos, pela computação em nuvem (cloud computing), pela internet das coisas (IoT),pela Internet Indústrial das coisas (IioT), pelos softwares de integração e gerenciamento de recursos das empresas (ERP), pelas inovações em tecnologia da informação e comunicação (ICT), pela

155 Consulta e Audiência Públicas nº 16/2020. Disponível em: < http://www.anp.gov.br/consultas-audiencias-publicas/concluidas/5997-consulta-audiencia-publica-n-16-2020 > Acesso em 14 de novembro de 2020.

identificação por intermédio de rádio frequência (RFID) por tecnologias de proteção de dados, dentre outras. A chamada Indústria 3.0 a precedeu a Indústria 4.0 e se caracterizou pela automação de processos e máquinas; assim, a Indústria 3.0 promoveu a introdução de processos e técnicas digitais em sistemas analógicos e nos complexos fisicamente estruturados, possibilitando uma integração e a formação de um ambiente produtor de informações e dados e um substancial aperfeiçoamento de toda a cadeia de valor da indústria.(MOHANTA et al, 2020)

Nesse sentido, a Indústria do Petróleo 4.0 apresenta as possibilidades de inovação tecnológica em cada um dos segmentos upstream, midstream e downstream. Neste texto, algumas aplicações das tecnologias da indústria 4.0 serão apresentadas, organizadas em atividades desenvolvidas nos segmentos da indústria do petróleo; em que pese as aplicações aqui apresentadas ainda representarem os primeiros protótipos do que será implantado em larga escala nos próximos 10 anos.

No segmento upstream, a exploração de petróleo no mar envolve riscos e incertezas. Um exemplo destas incertezas ocorreu no Brasil, na década de 2000, quando a Petrobrás já realizava há anos estudos geofísicos e geomorfológicos do campo de Parati. A exploração obteve resultados positivos mas exigiu gastos superiores aos que, preliminarmente, foram encontrados. Os resultados avaliados como viáveis em escala somente vieram com o campo de Tupi. Os estudos sobre reservatórios abaixo da camada pré sal, a 7000 metros de profundidade, em condições de temperatura e pressão específicos e com riscos operacionais significativos e custos elevados.

Os estudos geológicos de maior contribuição para o processo são a geologia estrutural, que investiga falhas, anomalias estruturais e fraturas; a sedimentologia, na análise de estratos sedimentares, realizados por intermédio de dados coletados por tecnologias de sismologia, e perfuração a grandes profundidades; a estratigrafia, que se caracteriza pelas técnicas que permitem avaliar as rochas sedimentares em uma moldura espaço-temporal; e, a geoquímica, com tecnologias de avaliação sobre o potencial do conteúdo dos reservatórios em termos de petróleo e gás. Os dados sísmicos da exploração de petróleo na camada pre sal foi feita com tecnologia 3D para imageamento. Contudo, a tecnologia 4D tem se desenvolvido, principalmente, em duas vertentes: nas tecnologias baseadas na detecção de mudanças, e naquelas baseadas na detecção temporal de alterações (travel-time changes). Com efeito, existem distintas técnicas de prospecção sísmica, mas o método da reflexão é o mais difundido na indústria. Por meio dele os dados sísmicos obtidos na prospecção são processados por supercomputadores que produzem imagens da subsuperfície com definição precisa das formações propícias à acumulação de hidrocarbonetos (ROBINSON e TREITEL, 2008).

Todavia, mesmo as melhores técnicas geológicas e geofísicas não substituem o papel desempenhado pela perfuração. Elas são fundamentais para ajudar a definir onde há maior potencial e apontar a melhor localização para a perfuração dos poços exploratórios e de avaliação.

A Indústria do Petróleo, nos três segmentos que a compõem, particularmente offshore, é um ramo de atividade de tecnologia de ponta. Perfurar poços em águas profundas, sob condições físicas exige uma engenharia altamente especializada e uma capacidade de integração de sistemas e tecnologias de diversas áreas. Este é o setor que demanda por inovação para superar os desafios que se apresentam. Exploração de petróleo e gás nos fundos oceânicos, em profundidades abaixo de 3000 metros de profundidade, com perfurações que ultrapassam os 3000 metros, a uma distância de mais de 150 milhas náuticas de terra (aproximadamente 300 km) é um desafio que impõe o emprego de alta tecnologia.

3. BIG DATA[156] E CIBERSEGURANÇA NA Indústria DE PETRÓLEO E GÁS 4.0

Uma das características da Indústria 4.0 é a produção e tratamento de Big Data, muitas vezes não tratados, e dos quais buscam-se informações para o processo de tomada de decisão. o edital Petrobras-SEBRAE 2020-1[157], chamada pública de projetos de inovação realizada em realizada em 08 de maio de 2020, teve por objetivo identificar, selecionar e apoiar nos aspectos técnicos e financeiros projetos de inovação nas seguintes verticais tecnológicas: Tecnologias Digitais; Robótica; Tecnologia de Inspeção; Corrosão; Eficiência Energética; Modelagem Geológica; Redução de Carbono; Catalisadores; e, Tratamento de Água.

Destas, a que enfrenta os desafios tecnológicos específicos de Big Data é a que está relacionada à vertical tecnológica "Tecnologias Digitais", especificamente nos seguintes desafios: quantificar os impactos socioambientais decorrentes de vazamento de hidrocarbonetos líquidos e dos procedimentos de resposta com dispersantes químicos; otimizar a gestão de risco de unidades operacionais através do controle das ações mitigadoras desde a fase de projeto até a operação; e estimar a oferta e a tarifa de energia elétrica dinamicamente através da análise de várias fontes de dados do setor. Esta última combinando Big Data, Data Lake[158] e Machine Learning[159].

A Indústria do Petróleo 4.0 produz interpretações geofísicas, sísmicas, registro de poços, registros de produção, modelos de reservatórios, dados de perfuração e muitos outros em tempo real. Na exploração de petróleo e gás offshore, a capacidade de armazenar e tratar esses grandes volumes de

156 O termo "Big Data" refere-se a conjuntos volumosos de dados. O tamanho das bases de dados geralmente atinge a ordem de Exabyte que equivale a 1024 Petabyte, ou seja, são bases realmente muito grandes, pois ultrapassam a 1 Bilhão de Gigabytes.

157 Disponível em: < https://www.sebrae.com.br/Sebrae/Portal%20Sebrae/Anexos/2020-05-08%20Edital%20Petrobras-Sebrae%202020_RevFinal%20Para%20Portal.pdf > acesso em 20 de novembro de 2020.

158 Data Lake é um repositório de dados armazenados em seu formato natural, geralmente formado por objetos blobs ou arquivos. O Data Lake armazena todos os dados corporativos, incluindo cópias brutas dos dados do sistema de origem e dados processados como relatórios, visualização, análises e dados de machine leraning. Inclui dados estruturados, semi-estruturados, não-estuturados e binários.

159 Machine learning é um subcampo da engenharia e da ciência da computação que trabalha o reconhecimento de padrões e a teoria do aprendizado computacional em inteligência artificial.

dados está sujeita a três variáveis que impõem a tecnologia Big Data: o volume de dados, a velocidade com a qual são produzidos, e a variedade de formatos e de estruturas de dados como são gerados.

A Indústria do Petróleo 4.0, em função dos avanços tecnológicos de procedimentos e equipamentos para coleta de dados sísmicos, vibracionais, de mecânica dos fluidos, de medição de perfis geofísicos e geomorfológicos de poços de petróleo houve uma aumento significativo do volume de dados. Por isso, as técnicas de análise de Big Data substituem as anteriores, que já não atendem às necessidades da atividade. Isso, no caso específico de upstream.

No segmento de midstream, as análises de Big Data podem reduzir os custos de operação e a redução de emissões de dióxido de carbono e óxidos de enxofre no transporte marítimo[160]. Da mesma forma, o monitoramento e análise de danos em dutos produzem grandes massas de dados neste segmento da Indústria do Petróleo 4.0. Essas análises além de possibilitar a localização de vazamentos, permitem estudos preditivos e de confiabilidade de pipeline[161].

No segmento de downstream, a tecnologia Big Data pode otimizar o gerenciamento em larga escala de ativos de Petróleo e Gás. O mercado desse tipo de ativos possui elevado grau de volatilidade, e a análise de dados financeiros do mercado de energia demanda esse tipo de capacidade de gerenciamento de Big Data. A tecnologia pode contribuir diretamente nos mercados de ativos, na distribuição, no mercado de petróleo, gás e derivados assim como afetar a economia do país, por fazer parte de agregados macroeconômicos, na sociedade como um todo.

3.1 Big Data e cibersegurança no segmento upstream da Indústria de Petróleo e Gás 4.0

É inegável que o interesse competitivo no mercado de petróleo e gás, o valor das expectativas no mercado financeiro e os interesses estratégicos para os países dessa indústria levam, necessariamente a uma análise de risco e de vulnerabilidades de cibersegurança. Porém, o maior risco na exploração offshore são os acidentes e vazamentos, particularmente na exploração de reservatórios na camada pré-sal a 7000 metros de profundidade, em condições de operação de difícil monitoramento, onde há

160 As emissões do transporte marítimo afetam o meio ambiente, o clima e a saúde humana. As emissões incluem gases relacionados ao clima, como dióxido de carbono (CO2), metano (CH4) e óxido nitroso (N2O) e hidrocarbonetos halogenados. As emissões de óxidos de enxofre (SOx) e óxidos de nitrogênio (NOx) contribuem para a acidificação de áreas marítimas e para a formação de partículas secundárias. O NOx contribui para a eutrofização. SOx, NOx e a emissão de partículas têm impacto negativo na saúde humana podendo levar a doenças respiratórias e mortes prematuras por doenças cardiopulmonares. Diferentes tipos de partículas têm impactos diretos e indiretos no clima. A MARPOL 73/78, Convenção Internacional para a Prevenção da Poluição por Navios, da Organização Marítima Internacional (IMO) regula a poluição do ar e as emissões de partículas. (SALO et al, 2016)

161 Pipeline, neste contexto são oleodutos ou gasodutos.

dificuldade de uma consciência situacional e, portanto, tornando a tomada de decisão em circunstâncias com maiores incertezas.

No segmento upstream, os riscos de cibersegurança se dão em função da espionagem Indústrial, seja com relação aos dados de geofísica e geomorfologia, informações sobre levantamentos sobre símica de reservatórios nos fundos oceânicos, bem como georreferenciamento de pesquisas geológicas, pelo valor de mercados das expectativas relacionadas ao empreendimento.

Um exemplo recente foi um fato decorrente a ataque cibernético, publicado no site CISO ADVISOR em setembro de 2020, que dá conta que um cibercriminoso propôs a comercialização, na dark web, de informações sobre vulnerabilidade que supostamente poderia dar acesso a redes da Petrobrás e da Agência Nacional de Petróleo (ANP), sendo que o valor cobrado pelo hacker foi de US$ 11 mil para os dados de acesso da Petrobrás e para a rede da ANP US$ 2 mil, para depósito por meio de bitcoins. (CISO ADVISOR, 2020)

Contudo, em que pese a fase de levantamento geomorfológico sempre ter apresentado um um risco de cibersegurança relativamente baixo, na Indústria do Petróleo 4.0 os dados produzidos por clusters de HPC (High-performance computing) a gerar grandes volumes dados tendem a aumentar significativamente esse risco. Além disso, a que se considerar que esse dados venham a alimentar as outras fases do segmento upstream, e considerando, também, que o uso de sensores em offshore leva à captação de dados em tempo real das atividades de exploração de petróleo e gás nos fundos oceânicos, esses grandes volumes de dados aumentam o risco de cibersegurança, pois o risco de um ataque cibernético podem levar a danos que podem inviabilizar o próprio projeto como um todo, como perfuração, estado geofísico das camadas perfuradas, estado dos elementos mecânicos, estimativas, dentre outros. No estágio de desenvolvimento do segmento upstream, as atividades de perfuração e o paralelismo entre elas, a diversidade de empresas realizando diferentes tarefas reveste a fase de complexidade pela dificuldade do estabelecimento de um protocolo de segurança a ser compartilhado por todos os envolvidos.

No estágio atual, a segregação das redes e a atuação em grandes profundidades, a mais de 300 km do litoral se constitui em uma barreira aos ataques cibernéticos. Porém, a Indústria do Petróleo 4.0 integrará as redes e subsistemas, permitindo um grau de controle e aproveitamento de Big Data jamais visto até então. Porém, ao mesmo tempo, aumenta significativamente os riscos em termos de cibersegurança. Quanto a fase de produção e fechamento de poço, fase final do segmento upstream, há que se considerar que a evolução da tecnologia ocorreu com a operação já iniciada, o risco se apresenta ainda maior, pois o planejamento do poço não considerou aspectos de segurança de dados, e a vulnerabilidade cibernética dessas instalações é significativamente maior.

Um exemplo de ciberataque foi o que ocorreu em 2012 com a empresa da Arabia Saudita chamada de “Saudi Aramco”. Esta empresa é uma das maiores petrolíferas do mundo. Um malware

denominado de “Shamoon” afetou cerca de 75% da estrutura de TI da empresa. As operações foram paralisadas. Ná época, um grupo que se autodenominava “Cutting Sword of Justice” teria reivindicado a autoria do ciberataque, querendo fazer supor tratar-se de um atentado. Contudo, especialistas da área de TI obtiveram fortes indícios para acreditar que se tratava de uma ação mais sofisticada. É possível que o Irã tenha utilizado o ciberataque à Arábia Saudita como retaliação ao Stuxnet [162]. A consequência econômica não atingiu somente aos Estados Unidos, mas a todo o mercado de petróleo e gás.

Desta forma, conclui-se que, se uma parte significativa do mercado de petróleo e gás materializa-se no mercado de futuros, onde há comercialização de títulos financeiros que projetam expectativas, então um ataque cibernético a bases “big data” se tornam críticas e impõem aperfeiçoamento de mecanismos de cibersegurança, especialmente no segmento upstream.

3.2 Big Data e cibersegurança no segmento midstream da Indústria de Petróleo e Gás 4.0

Cabe ressaltar que dados do segmento midstream são do interesse competitivo. O setor midstream tem seus principais aspectos no modal de dutos e no transporte marítimo (shipping), este último será explorado em tópico específico.

A Resolução nº 810/2020 da Agência Nacional do Petróleo, Gás Natural e Biocombustíveis (ANP), especificamente sobre a gestão de segurança operacional de terminais para movimentação e armazenamento de petróleo, derivados, gás natural e biocombustíveis, instituiu procedimentos nos termos do “Regulamento Técnico de Terminais para Movimentação e Armazenamento de Petróleo, Derivados, Gás Natural e Biocombustíveis” (RTT). Diz o art. 4:

> É obrigação dos titulares de autorização outorgada pela ANP: inciso III - assegurar o livre acesso às instalações do terminal e às operações em curso, para fins de: d) levantamento de dados e informações e apuração de responsabilidades sobre
>
> incidentes operacionais ocorridos nas instalações sujeitas ao RTT.

162 Stuxnet é um worm de computador projetado especificamente para atacar o sistema operacional SCADA desenvolvido pela Siemens e usado para controlar as centrífugas de enriquecimento de urânio iranianas. Foi descoberto em junho de 2010 pela empresa bielorrussa desenvolvedora de antivírus VirusBlokAda. É o primeiro worm descoberto que espiona e reprograma sistemas Indústriais. Ele foi especificamente escrito para atacar o sistema de controle Indústrial SCADA, usado para controlar e monitorar processos Indústriais.

O que, implicitamente, impõe a armazenagem de dados de dutos. Na Indústria do Petróleo e Gás 4.0 esse volume de dados, conforme já dito, podem chegar a bases muito extensas e a necessidade de ferramentas de manipulação de Big Data.

Um outro efeito é a discrepância entre os dados de midstream e upstream o que afeta negativamente o mercado, gerando incertezas e externalidades negativas, impactando expectativas e causando anomalias nas operações de ativos.

Por esses motivos, e outros de caráter técnico, e considerando a proteção do meio ambiente, a proteção contra ataques cibernéticos das redes de dados (e mesmo os próprios dados) da rede de dutos emerge como fator da maior importância. Sem contar, segundo uma análise consequencialista, os danos à terceiros em virtude de interrupções (custos), e as implicações à plantas (refinarias), equipamentos e sistemas.

O sistema de gerenciamento de software de dutos é comumente construído em sistemas de controle de supervisão e aquisição de dados (SCADA) que permitem aos operadores monitorar e controlar muitos aspectos das operações. Os benefícios do sistema SCADA são reduzir os custos operacionais e melhorar a eficiência do sistema. No entanto, os hackers podem tirar vantagem do sistema SCADA para interromper os serviços de dutos e causar derramamentos, explosões ou incêndios.

3.3 Big Data e cibersegurança no segmento downstream da Indústria de Petróleo e Gás 4.0

O risco operacional no segmento downstream se relaciona à grande diversidade de dispositivos e estruturas de uma planta de processamento de petróleo e gás. Na Indústria de Petróleo e Gás 4.0 os sensores e unidades de automação, seja em instalações de refino, de armazenagem ou distribuição são complexificados com o uso de Big Data e Blockchain, como ocorre, por exemplo, em processos de alta pressão, temperaturas elevadas e combustíveis altamente inflamáveis. Os compressores, as bombas, os geradores de energia elétrica, as máquinas auxiliares e os dispositivos de automação, válvulas, sensores, monitores de destiladores, e outros dispositivos de uma refinaria de derivados de petróleo e gás apresentam complexa conexão e são suscetíveis a ciberataques, seja para a coleta de dados, seja para atentados.

Os algoritmos, protocolos, redes e servidores dedicados devem possuir capacidade de interoperabilidade a fim de evitar falhas operacionais. Quando um sistema gerenciador de Banco de Dados centralizava aplicações, provia uma camada lógica de compatibilidade que facilitava a interligação de aplicações mas vulnerabilizava o sistema. As soluções de IioT baseadas em Blockchain com arquitetura distribuída e encriptada traz à Indústria do Petróleo e Gás 4.0 uma inovação disruptiva que ainda não se vislumbra em todas as suas possibilidades.

Um desses efeitos decorrentes é a redução da intervenção humana nos processos e o desenvolvimento de algoritmos de inteligência artificial, machine learning, e outras tecnologias que exigem qualificação e especialização dos colaboradores, contudo, esses ainda são a maior vulnerabilidade à ataques cibernéticos.(NGUYEN et al, 2020)

Segundo o site especializado CISO Advisor, informações publicadas em outubro de 2020 dão conta que ao longo dos primeiro semestre de 2020 os ataques cibernéticos a sistemas do setor de petróleo e gás aumentaram em relação a todo ano de 2019. Ainda segundo os editores do site os ataques contra instalações Indústriais tendem a se apresentar especialmente danosos. Os objetivos dos hackers não se restringem, somente, aos ganhos financeiros, mas também a ciberespionagem. No setor de petróleo e gás, a porcentagem de computadores de ICS nos quais foram bloqueados objetos maliciosos aumentou de 36,3%, no segundo semestre de 2019, para 37,8%, no primeiro semestre de 2020.

É fato que o setor de logística apresenta riscos de natureza distinta, sendo afetados por operações de detecção de falhas, manutenção de itens críticos e aquisição de sobressalentes para manutenção. A tecnologia contribui para a eficiência e aumento da disponibilidade de equipamentos e confiabilidade. Contudo, as atividades do varejo continuam inseguras, o que sofrerá verdadeira “virada de Copérnico” co o uso de criptoativos e pelas transações com o uso de criptomoedas.

Contudo, questões de privacidade, proteção de dados pessoais e mesmo de internacionalização de mão de obra serão impactados pela tecnologia na Indústria do Petróleo e Gás 4.0. Como conclusão parcial podemos afirmar que o processo de internacionalização, com a participação de empresas de diferentes nacionalidades, inclusive na complexificação da cadeia de suprimentos será dependente de modelos de previsão e controle de estoques a serem fortemente baseados em Big Data.

Noutro sentido, o direito da tecnologia será instado a oferecer soluções ao ordenamento jurídico, no sentido de proteção de privacidade de dados, principalmente em função de tecnologias de Data Analytics[163] na Indústria do Petróleo e Gás 4.0.

A base de dados distribuída trará demandas de Tecnologia da Informação (TI) no sentido de submeter a sistemas de segurança cibernética, protocolos, algoritmos específicos de conformidade, técnicas de redes inteligentes, criptoanálise com chaves mais robustas e soluções de inteligência artificial para análise de comportamentos de ameaças, toda uma complexa engenharia de cibersegurança para fornecer suporte à Indústria de Petróleo e Gás 4.0.

O “core” das iniciativas se concentrará na convergência e interconectividades de sistemas, no gerenciamento de cripto ativos, no aproveitamento de sistemas mais antigos em um período de transição,

163 Data Analytics são as técnicas de análise de dados de diferentes estruturas com o propósito de identificar padrões e estabelecer relacionamentos que se consubstanciem em conclusões sobre tendências, anomalias, padrões, comportamentos, funções, e informação utilizável na tomada de decisões

no qual a criticidade das soluções se apresentará mais vulnerável á ataques cibernéticos. Os esforços se complexificam quando essas tecnologias, as mais diversas, com padrões os mais distintos, fornecendo outputs de formatos e estruturas de dados diferentes precisam ser conectados. Essa transição da tecnologia da informação da Indústria do Petróleo e Gas 4.0 pode ser categorizada por esforços em três frentes tecnologia operacional ou operational technology [164] (OT), tecnologia da informação (TI) e a Internet Indústrial das Coisas (IioT). Essa exigência de conectividade entre sistemas e protocolos, considerando a produção de grandes volumes de dados, nesse caso big data, além de riscos cibernéticos há riscos operacionais relevantes.

4.0 A TECNOLOGIA BLOCKCHAIN NA INDÚSTRIA DO PETRÓLEO E GÁS 4.0

É intrínseco a qualquer indústria da revolução 4.0 o uso da tecnologia Blockchain. Contudo, dadas as condições extremas nas quais a Indústria de Petróleo e Gás 4.0 offshore opera, a tecnologia se constitui em condição inafastável para a estruturação do setor.

4.1 Blockchain

Pode-se dizer, sem um compromisso rigoroso, que a tecnologia Blockchain surgiu em 2008. Nesse período, a tecnologia passou por muitos aperfeiçoamentos; contudo, pode-se dividir em três fases importantes: uma primeira, caracterizados pelo Bitcoin [165]; em uma segunda, pelo marcada pelo Ethereum[166]; uma terceira etapa, dos smart contracts[167], e a quarta do Ethereum 2.0[168].(LU et al, 2019)

Preliminarmente, o conceito se apresenta de muitas formas. Em uma conceituação simples, trata-se de uma estrutura de dados, uma cadeia de pedaços criptografados de estrutura de dados de tal complexidade que, mesmo diante de tecnologias muito poderosas, seria pouco provável uma quebra de segurança. Portanto, do ponto de vista funcional, é uma estrutura de dados de difícil adulteração ou

---

164 Operational Technology (OT) compreende hardware e software sensíveis às variações ou as provocam , por intermédio de monitoramento direto e/ou controle de equipamentos; atuando sobre o a partir de ativos, processos e eventos da indústria. OT inclui Indústrial control system (ICS) como, por exemplo, Supervisory Control and Data Acquisition (SCADA), programmable logic controller (PLC), remote terminal unit (RTU), distributed control system (DCS), dentre muitos outros.

165 Bitcoin é uma cripto moeda que utiliza a tecnologia Blockchain e se baseia em um processo chamado mineração de dados.

166 Ethereum passou a adotar o paradigma de que toda transação, registro, execução de código distribuído, assinatura digital, ou qualquer outra aplicação que seja executada na rede do Ethereum seja paga em ether, sendo assim, o Ethereum pode ser visto como um grande computador de escala global, no qual usuários pagam pela quantidade de recurso utilizado.

167 Smart Contract, ou contrato inteligente são contratos digitais, um programa autoexecutável desenvolvido para facilitar, efetivar e proteger as operações financeiras de Blockchain.

168 Ethereum 2.0 entrou em operação dia 01 de dezembro de 2020 e materializa a mudança do “esquema de validação” das transações da blockchain do Ethereum. A transição é do Proof of Work(PoW), primeiro protocolo de consenso, para o Proof of Stake(PoS), que foi criado para reduzir custos, cuja premissa básica é economizar os equipamentos de mineração de blocos(muito caros), e passar a adquirir em cada nó “validador” da rede as moedas do sistema específico de blockchain.

fraude, e com a qualidade de poder ser rastreada em um ambiente de rede peer to peer (P2P)[169]. (AHMED & KHAN, 2020)

É produto de tecnologia que combina computação, tratamento de dados distribuídos, ambiente de rede de conexão peer to peer, criptografia e mecanismos de consenso. A inovação mais significativa, dentre tantas, que a tecnologia blockchain trouxe foi o tratamento de dados distribuídos e rastreáveis, deixando para trás a ideia de armazenamento em banco de dados.

O ambiente de rede não é centralizado em um servidor, pois em cada nó da rede há máquinas rodando com um mesmo status, justamente no critério P2P. Assim, os nós da rede compartilham recursos/informações por intermédio de protocolos próprios.

O que mudou com o uso de Blockchain? Anteriormente, as transações passavam por um crivo de um órgão centralizador, que certificava e, inclusive, armazenava os dados. Com a tecnologia de Blockchain, as transações são estabelecidas diretamente entre as partes, sem a intervenção de um terceiro. Os dados da transação encontram-se na própria estrutura Blockchain, de forma distribuída. Ora, nesse caso, como se dá a certificação da informação de um Blockchaim, se não há mais uma autoridade, um terceiro mediando a transação? Isso se dá por "algoritmos de consenso"[170].

Dinâmica de transações com Blockchain: Dado que dois indivíduos manifestam interesses recíprocos de estabelecer uma transação com o uso de Blockchain, ambos utilizam os dados relacionados à transação como uma variável e o fazem buscando estabelecer a transação utilizando um ambiente comum, nesta mesma moldura temporal e, assim, formar um "bloco de dados", uma "cadeia de blocos de informações". A transação é criptografada e distribuída para a rede no modo P2P. No computador o "algoritmo de consenso" confirma (ou não) a transação; e, ao validá-la acrescenta um "Hash"[171] exclusivo daquele bloco de informações. Na ocorrência de qualquer discrepância, seja por que motivo for, o Hash correto não poderá ser confirmado e um erro será relatado, isso confere confiabilidade à estrutura. Ambos os blocos de informações de cada um dos dois indivíduos que realizam a transação são "confrontados"; e, havendo compatibilidade, esses blocos formam uma "cadeia de blocos" (Block chain) e a transação com ela realizada, segura, criptografada e validada. A tecnologia Blockchain usa estratégias de armazenamento distribuído o que protege contra fraudes cibernéticas. Na

169 Rede peer-to-peer (P2P) é, a grosso modo, um ambiente no qual os computadores que ocupam cada nó da rede possuem o mesmo status, cada nó tem a mesma alimentação de rede e não há servidor centralizado. Todos os nós compartilham recursos ou informações por meio de protocolos específicos.

170 "Algoritmo de Consenso" é um software que oportuniza a cada rede Blockchain chegar a um acordo(consenso). As redes públicas descentralizadas de Blockchain são construídas segundo a arquitetura de sistemas distribuídos e, como não há uma autoridade central certificadora, os computadores da rede precisam concordar na validação das transações. Os algoritmos de consenso garantem que as regras do protocolo estão sendo seguidas e que todas as transações ocorrem de forma confiável.

171 A função Hash (Resumo) é qualquer algoritmo que mapeie dados grandes e de tamanho variável para pequenos dados de tamanho fixo. Por esse motivo, as funções Hash são conhecidas por resumirem o dado. O algoritmo de hash, em se tratando de Blockchain, possui técnica de criptografia.

Indústria de Petróleo e Gás 4.0, o blockchain traz um diferencial tecnológico, particularmente, quanto à tomada de decisões, nas transações comerciais, no gerenciamento e na segurança de dados.

Inciando pelo diferencial trazido na tomada de decisões, alguns problemas afetos à E&P de petróleo e gás, estão relacionados ao projeto, como varredura tridimensional de dados de reservatórios, implementação da estrutura de poço, e manutenção de equipamentos. O processo se estende por muito tempo, desde os estudos de viabilidade até a implementação e testes. No projeto, a tecnologia Blockchain protege dados relevantes, fornece registros inalteráveis e facilita a consolidação de informações confiáveis. O processo decisório segue um ciclo que é alimentado por informações, e quanto mais rápido esse processo "girar", mais eficientes são as decisões, mais rápido se passa a fase seguinte, maior é a vantagem competitiva. Assim o Blockchain possibilita um sistema autônomo, com estrutura, protocolo e interoperável, permitindo transmissão de dados confiáveis e precisos, evitando fraudes e melhorando a cibersegurança. Esse processo, no mais das vezes é descentralizado, e o uso de smart contracts confere eficiência ao processo. O resultado do processo é rapidamente publicizado, o que impacta no mercado em função da rapidez, afetando assimetrias de informação e expectativas. Nas transações comerciais, há que se considerar a cadeia de valor da Indústria de Petróleo e Gás nos segmentos upstream, midstream e downstream.

No segmento upstream há o maior retorno de valor, com os maiores ganhos por barril/m³ produzido. A dinâmica do segmento pressupõe um aumento progressivo de investimentos a medida que a produtividade decresce, com o propósito de manter os níveis de produção. Os riscos desse segmento são as variações de preços no mercado, incertezas nas relações internacionais e operacionais, estes últimos ligados à danos ambientais. O segmento midstream tem sua cadeia de valor caracterizado pelo transporte de petróleo e gás até pantas de processamento e distribuição. Inclusive pelo mercado de Brent[172]. Neste assunto das transações comerciais o contrato é o instrumento intensamente utilizado. A tecnologia Blockchain se apresenta no segmento midstream por intermédio de smart contracts e suas possibilidades. Apesar das vulnerabilidades inerentes às tecnologias de dados, que importa em esforços de auditoria, a ocorrência de fraudes e perdas por atividades ilícitas ou ao arrepio de contratos firmados podem ser significativamente reduzidas. A redução de instrumentos e a simplificação de procedimentos tendem a melhorar a eficiência das transações.

O segmento downstream é uma parte da cadeia de valor que mais diversifica a emissão de papeis e a geração de fluxo de caixa na Indústria de Petróleo e Gás. O varejo e o mercado de derivados, a distribuição e o planejamento tributário representam oportunidades para o uso de Blockchain pela emissão de criptoativos e pela implementação de um novo mercado que ainda carece de regulamentação no Brasil. As transações mais rápidas e seguras podem alavancar hedge e mercados de futuros. As escala

172 Brent é uma forma de se referir ao petróleo cru, ainda não beneficiado, que se subdivide em Brent Crude, Brent doce leve, WTI, e outros padrões de benchmark.

das transferências internacionais na Indústria de Petróleo e Gás feitos em criptomoedas tendem a reduzir os custos de transação e otimizar a eficiência de fundos.

Cotação do Bitcoin em US$. Fonte: https://www.tradingview.com/x/PzZNxeM7/

Quanto ao gerenciamento da Indústria de Petróleo e Gás, o uso da tecnologia Blockchain pode oportunizar análises mais precisas em tempo real e mecanismos de intervenção mais eficazes. O segmento de maior complexidade de gerenciamento é o de midstream, particularmente o sistema de dutos, informações sobre estados e sinais analógicos de interesse da operação, melhorando aspectos de manutenção e confiabilidade.

Ainda no setor de midstream o rastreamento de produtos na cadeia de suprimentos, o pedido e fornecimento de itens de manutenção, e demais aspectos de logística podem melhorar sua eficiência com o uso de Blockchain. Outro aspecto de interesse de interesse na Indústria de Petróleo e Gás 4.0 offshore é o controle da propriedade intelectual e sua proteção. Custos de conformidade, bem como de propriedade, de assinaturas, de certificação, todos são otimizados pelo uso de Blockchain.

No que diz respeito à segurança cibernética, a Indústria de Petróleo e Gás vem, até agora, sofrendo um volume significativo de ataques cibernéticos. Segundo o site especializado CISOADVISOR[173], de setembro de 2020, redes da Petrobrás e da Agência Nacional de Petróleo (ANP)

173 CISO Advisor é um website dedicado à segurança cibernética, segurança da informação e ciberdefesa, focado no interesse dos profissionais de segurança – incluindo administradores de rede, administradores de data center e outros, mas principalmente aos chief information security officers (CISOs), profissionais que estão

podem ter se tornado alvos de intrusões por parte de um cibercriminoso, que estaria comercializando, na dark web, informações sobre vulnerabilidade que, segundo o criminoso, teria a capacidade de conceder acesso às mesmas. A notícia dá conta que o hacker estaria cobrando, pelos dados de acesso à redes da Petrobrás, o valor de US$ 11 mil, e para as redes da ANP o valor de US$ 2 mil, com depósito em bitcoins.

A Indústria de Petróleo e Gás possui uma vasta gama de vulnerabilidades para uma ameaça cibernética, como sistemas de alta complexidade com produção de grande bases de dados, particularmente no segmento upstream, e baixo índice de interoperabilidade entre os sistemas de produção e os sistemas de processamento de informações, um significativo delay entre a análise de dados operacionais e a produção de informações confiáveis para o processo de toma de decisões, possibilidade de processamento de inconsistências, incompatibilidades entre redes, entre outros riscos ligados à tecnologia da informação.

A Indústria de Petróleo 4.0 com a tecnologia Blockchain conferem um grau de segurança até então inimaginável, por sua arquitetura distribuída, pelos sistemas de autenticação, pela criptografia de elevada complexidade, dentre outros aspectos técnicos, reduzem o riscos de ciberataques.

4.2 IoT e a tecnologia Blockchain na Indústria de Petróleo e Gás 4.0

A Indústria de Petróleo e Gás 4.0 experimenta, no momento uma complexificação nas Tecnologias da Informação e Comunicação (TIC) e os preços no mercado internacional estabilizaram após uma queda pouco significativa. O fato é que a internet das coisas IoT contribuem de forma relevante o uso de tecnologias como computação em nuvem, inteligência artificial, block-chain, Big Data, dentre outras.

Indústria 4.0 e Internet das Coisas - IoT são termos utilizados no mercado de soluções integradas que referem-se ao tratamento de dados com ferramentas tecnologicamente mais ágeis e com maior capacidade de integração e automação. Esse ambiente tecnológico acaba por conectar sistemas ciberfísicos, Internet das coisas, computação em nuvem e computação cognitiva.(SINGH et al, 2020)

O desenvolvimento está ocorrendo de tal forma que certas infraestruturas baseadas em nuvem incluem o ambiente de Internet das coisas (IoT), este arranjo estabelece uma relação entre os ambientes conectados, os dados que são produzidos ou trafegam nas redes, tendo sido originados nas atividades da Indústria do Petróleo de Gás 4.0, são incorporados por intermédio de sensores, outros sistemas, e mesmo RFID, e todo esse contexto fica armazenado na nuvem.

---

no topo da cadeia de comando e desempenham papel crucial na segurança cibernética e da informação, bem como no desenvolvimento e aprimoramento de políticas e programas de proteção de dados corporativos.

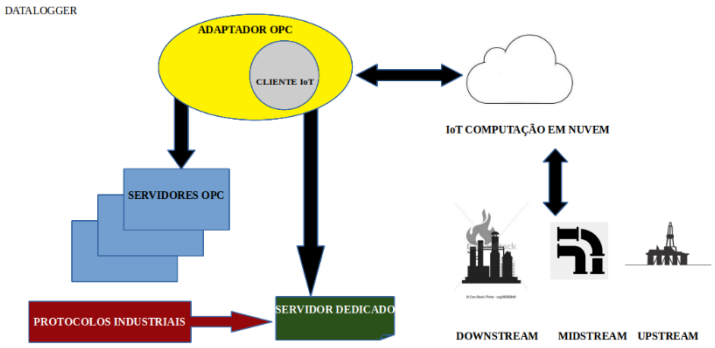
Um sistema de internet das coisas, IoT, passa necessariamente por três estágios: a implantação, que compreende o planejamento, estruturação, implantação, coleta de dados e primeira entrega de resultados; a partir daí, há uma ênfase na inteligação de estruturas horizontais e integração dos sistemas de acesso; e, por último, o sistema deve integrar todos os dados em sistemas de computação na nuvem (Cloud Computing) e prover um compartilhamento de dados para gerenciamento de operações.

Na Indústria de Petróleo e Gás 4.0, a sofisticação dos sistemas SCADA, protocolos de comunicação específicos como OPC, e a integração destas estruturas coma IoT e tecnologias de Cloud Computing, produzem resultados em escala tão significativos que representam verdadeira revolução tecnológica na E&P. Por intermédio da IoT pode-se implementar modelos de previsão, detectar tempos de inatividade e reduzi-los, realizar manutenções corretivas, e melhorar a eficiência do sistema como um todo. (SURESH et al, 2020)

Para que esse contexto seja implementado com um grau de segurança aceitável, há a necessidade de protocolos de segurança cibernética e o tratamento de grandes volumes de dados (Big Data), principalmente em função das soluções de Cloud Computing. (TYAGI & KUMAR, 2020)

Muitos são os dispositivos que produzem um sensoriamento remoto das operações, para permitir o acesso aos dados de pressão e fluxo, como: automação de elementos de poço; dados específicos da geofísica do reservatório; dados sobre o estado dos dutos; controle eletromagnético para se evitar a ocorrência de concentração de cargas e o risco de descargas elétricas; dentre muitas outras.

Na figura 1 exemplifica-se um modelo possível de solução de IoT na Indústria. 4.0



ARQUITETURA DE SISTEMA DE DADOS DE IoT NA INDUSTRIA DO PETRÓLEO E GÁS 4.0

Fig. 1 Data Logger[174] adaptado TOMA & POPA, 2018, p.48

De uma maneira simplificada, um sistema de IoT na Indústria de Petróleo 4.0 teria, ao menos, os seguintes componentes:

i. Sensor de Torre de Destilação, que modela o comportamento de uma unidade de destilação de petróleo bruto, incluindo dados de temperatura e de produção.
ii. Banco de Dados para IoT Cloud, com o propósito de armazenar e disponibilizar dados na nuvem dos sistemas em operação em tempo real, principalmente de pressão, o mais crítico.
iii. Um gateway[175] de IoT para OPC [176], OPC UA[177], e integração de arquiteturas. (ALAM et al, 2020)

A aplicação aqui exemplificada é baseada em Banco de Dados, mas poderia não ser. Neste caso, esse gerenciador de base de dados é o principal componente na armazenagem de dados de sensores Indústriais, podendo valer-se de estruturas de dados específicas para interagir com diferentes aplicativos corporativos, com a necessidade de conectividade a redes dedicadas. O sistema precisa ser equipado com software de mineração de dados, de computação distribuída, de computação em nuvem, algoritmos de Data Analitics, Dashboard[178] , e outras tecnologias que se encontrem no "estado da arte".

174 Data Logger é um sistema que capta sinais analógicos de uma planta ou equipamento, como temperatura, pressão, umidade, vibrações mecânicas, emissões eletromagnéticas, variações sísmicas, luminosidade, dentre outras. Ou seja, um Datalogger é um sistema de coleta de dados Indústrial, com controle de gerenciamento de OEE, dados de produção por turno, controle de metas, apuração de resultados, dentre outras funcionalidades. Um datalogger pode, também, controlar o consumo de energia por peça produzida.

175 Gateway é um termo dado a um dispositivo eletrônico que cumpre uma função em uma rede de computadores. Cada rede de computadores possui um protocolo que é uma estrutura de dados com diversas funções no tráfego de informações nessa rede. Assim, um gateway pode compatibilizar protocolos de redes diferentes, pode traduzir protocolos, pode converter protocolos, sendo imprescindível para a interoperabilidade de sistemas.

176 OPC (OLE for Process Control), uma interface padronizada de comunicação que tem por propósito mitigar os problemas de compatibilidade entre dispositivos Indústriais de diferentes arquiteturas e fabricantes. Vale ressaltar que cada equipamento que possui software para funcionamento e possui um algoritmo de controle de funções chamado Driver. O OPC compatibiliza os diferentes "drivers". O OPC pode se apresentar com funções específicas: OPC DA (Data access) que estabelece a troca de dados; OPC A&E (Alarm and events) que serve para troca de informações de mensagem de alarme e evento, variabilidade e gerenciamento de estado; e, OPC HDA (Historical data access) para definir métodos de consulta e análises em dados históricos.

177 OPC UA (Unified Architecture) é um padrão de interoperabilidade para a troca de dados segura e confiável no espaço de automação Indústrial e em outras indústrias utilizado na Indústria 4.0, especificamente para compatibilizar IoT (Internet of Things), e IIoT (Indústrial Internet of Things).

178 Dashboard, em tecnologia da informação, consistem em um dispositivo de apresentação visual de um conjunto de informações e indicadores, que normalmente encontram-se distribuídos.

O funcionamento, em apertadíssima síntese, consiste no seguinte: Os dados obtidos a partir de sensores são transmitidos a um servidor OPC (baseado em OLE[179]) rodando no Data-Logger. Esses dados são armazenados em um gerenciador de banco de dados de IoT por intermédio de um OPC UA, e pela execução de um gateway Data-Logger. O servidor de OPC UA Server roda um gateway Data-Logger, e o OPC UA Client compatibiliza os dados obtidos dos sensores do gateway e armazena no gerenciador da base de dados de IoT, que envia para a nuvem (cloud computing[180]). A Indústria do Petróleo 4.0 utiliza esses dados e por intermédio de Data Analytics[181] processa as informações e realiza a tomada de decisões quanto a incidentes, produção, análise de previsibilidade, confiabilidade, otimização e outras. No caso dessa indústria o volume de dados se materializa no conceito de Big Data, já mencionado.

Conclusões

Assim, pode-se afirmar que a IIoT é imprescindível nas soluções para a Indústria do Petróleo 4.0, integrando aplicações, plantas, dispositivos, equipamentos, dutos, plataformas offshore, em todos os segmentos seja upstream, midstream ou downstream, compatibilizando dispositivos e protocolos de comunicação em rede. Ressalta-se a necessidade de técnicas de cibersegurança como requisito crítico em ambientes e infraestruturas suportadas por IIoT.

5.0 Tecnologia e a prevenção de fraudes marítimas no segmento downstream da Indústria de Petróleo e Gás 4.0

O conceito de fraude marítima, segundo o International Chamber of Commerce (ICC), do International Maritime Bureau (IMB):

> "Quando uma das partes intervenientes numa operação de comércio internacional – comprador, vendedor, armador, afretador, comandante do navio ou tripulação, segurador, banco, "broker" ou agente – consegue obter,

179 OEE (Overall Equipment Effectiveness) é um indicador utilizado em programas de TPM ("Total Productive Maintenance" arquitetura japonesa para minimizar perdas, reduzir paradas, assegurar qualidade e reduzir custos pela garantia de continuidade dos processos.) para medir eficiência, por isso ser denominado eficiência geral de equipamento, representando indicadores de disponibilidade, performance e qualidade.

180 Cloud computing, ou computação em nuvem é uma tecnologia que se baseia na utilização de dispositivos de armazenamento de dados, computação e conexão de servidores por compartilhamento e distribuição de tarefas e serviços por intermédio de princípios e arquiteturas da computação em grade. A funcionalidade mais imediata é a possibilidade de acesso a dados e serviços remotamente, a qualquer momento e a partir de qualquer lugar, sem a necessidade de programas específicos, tendo como método de conexão a interligação à intenet, dispensando o armazenamento local.

181 Data Analytics são as técnicas de análise de dados de diferentes estruturas com o propósito de identificar padrões e estabelecer relacionamentos que se consubstanciem em conclusões sobre tendências, anomalias, padrões, comportamentos, funções, e informação utilizável na tomada de decisões.

> de forma injusta ou ilegal, vantagem financeira ou apoderar-se de mercadorias em detrimento de outro participante que empreende a atividade comercial, de transporte ou obrigação financeira.” (tradução livre)

O custo das fraudes contra seguros, publicado pelas “Big Four Accounting Firms”[182] são, de fato, cifras significativas. Contudo, não se pode ter certeza do custo real dessas fraudes para a Indústria do Petróleo. Na verdade, pode ser muito mais alto. Isso porque não se consegue distinguir, pela análise de relatórios, se custos de investigação, custos da judicialização, custos de prevenção, dentre outros, estão contabilizados. O fato incontroverso, contudo, é que outras formas de agir desonestamente não são sequer detectadas, e quando o são, não são reportadas, o que torna muito difícil apurar-se o custo efetivo das fraudes. (SOYER, 2014)

O Allianz Risk Barometer: identificando os principais riscos de negócio para 2020 diz:

> O envolvimento de nações em ataques cibernéticos também representa um risco crescente para as empresas, que podem ser alvos de propriedade intelectual ou por grupos que pretendem causar interrupção ou danos físicos. As tensões no Oriente Médio fizeram com que os navios internacionais fossem atingidos por ataques no Golfo Pérsico. Instalações de petróleo e gás também foram afetadas. (ALLIANZ, 2020)

O que se pretende ressaltar neste texto é que a fraude ocorre em um ambiente no qual há alguns atores que participam da operação de transporte marítimo, operação que ocorre no segmento midstream da Indústria do Petróleo, e que estes atores possuem interesses, por vezes conflitantes, ou em circunstâncias nas quais há a possibilidade de custos menores, lucratividade maior, ou ambos; ainda que em detrimento de aspectos pactuados de determinada forma, em detrimento de, ou tendo como decorrência o dano de terceiros, maculando certos aspectos das transações.

5.1 O Blockchain na prevenção da fraude marítima

O uso da tecnologia Blockchain na prevenção da fraude marítima será um divisor de águas na proteção de direitos de propriedade, obrigações e deveres contratuais, atividades relacionadas com o transporte óleo; pois pelo antigo costume do transporte marítimo e seus tradicionais documentos sempre foram vulneráveis a fraudes. A tecnologia oportunizou que estes documentos sejam materializados em um novo formato, que permita à documentação novas possibilidades em termos de segurança e incorruptibilidade.

---

182 A expressão Big Four Accounting Firms, ou somente “Big Four”, é utilizada para fazer referência às quatro maiores empresas de serviços de auditoria do mundo, consistindo em Deloitte, Ernst & Young, KPMG e PricewaterhouseCoopers. São assim conhecidas por dominarem o mercado, por possuírem uma vasta gama de serviços em diversas áreas, e pela confiabilidade que gozam entre as maiores empresas do mundo.

Sobre esses documentos, o costume do transporte marítimo é tributário de uma tradição que há muitos anos se consolida neste ramo. Neste sentido, julga-se a necessidade de um escorço acerca desses instrumentos utilizados no transporte marítimo.

Segundo Osvaldo Agripino de Cartro Jr. o direito marítimo cincunscreve as normas que incidem sobre a navegação, o comércio marítimo, os contratos de transportes, seja pelo mar sejam pelas águas interiores; bem como direitos, deveres e obrigações dos atores envolvidos, sejam operadores ou interessados nos negócios, bem como na situação dos navios ou em suas operações.(CASTRO JR, 2004)

Assim, cabe explicar, em apertada síntese, os sujeitos envolvidos no transporte marítimo.

O proprietário é aquele que detém o respectivo título e seu registro. Inclusive, há a presunção da condição de proprietário daquele cujo nome consta do registro.(BRASIL, 1988, Art. 3 e 5)

O armador, que pode ser uma pessoa física ou jurídica, é aquele que equipa, que confere ao navio os acessórios necessários (inclusive a tripulação) ao que está sendo preparado para executar, ou seja, aquele que "arma" uma embarcação a casco nu. (BRASIL, 1997, Art. 2, Inciso III) Faz-se necessário pontuar que há a figura do armador-proprietário, que é o proprietário que, ele mesmo, arma o navio; assim como, quando o proprietário cede o navio para que outro exerça a náutica e a exploração negocial, este "outro" recebe o nome de armador-locatário.

Quanto ao frete, há o fretador, que cede o navio a fretamento; e, noutro polo, há o afretador, contratante de afretamento. Há outros partícipes subsidiários, que não serão tratados neste texto por escapar ao escopo do mesmo.

Contudo, há ainda o comandante, responsável pela técnica de navegação, pela carga, pela tripulação e demais assuntos ligados à operação do navio.(BRASIL, 2003, item 0401)

Quanto aos contratos, não todos, até porque tratativas não são limitantes, mas aqueles cujo costume do transporte marítimo consagrou, são os seguintes:

1. Voyage Charter Party (VCP), ou contrato de afretamento por viagem – considerando os direitos de usar, fruir e dispor. Assim, a fruição do navio consiste na percepção de benefícios que decorrem do aproveitamento negocial do que o navio pode trazer, que se materializa por intermédio dos contratos. Nesse sentido, no contrato de afretamento há um negócio entre o fretador e o ao afretador, que adquire o direito de fruição. No contrato de afretamento por viagem, o contrato existe, é válido e eficaz somente para uma determinada de rota, naquela determinada missão, que se inicia na instalação de carga, encerrando na instalação de descarga. Digo aqui "instalação" por aqui se tratar do segmento midstream, e nem sempre o óleo/gás serem carregados em instalações distintas de um terminal portuário.

2. Time Charter Party (TCP), ou contrato de afretamento por período, sendo aquele contrato com prazo de vigência. O afretamento por período, normalmente, se protrai no tempo, e a muitas viagens.
3. Bareboat Charter Party (BCP ou BBC) ou contrato de afretamento a casco nu - é um contrato mais abrangente em termos de domínio, pois tem por objeto a fruição e o uso. O afretamento tem a posse do navio, atrai a responsabilidade pela náutica (o que não acontece com nos modelos de contratos já mencionados VCP e TCP). O negócio proposto como afretamento a casco nu é firmado por longo prazo.
4. Contract of Afreightment (COA) como contrato de tonelagem é quase uma armadilha semântica, pois leva ao equívoco de ser um contrato de afretamento lato sensu. O operador (seja fretador ou transportador), por contrato, se obriga sobre uma carga, segundo um período e distribuído por navios, todos os aspectos estão reduzidos a termo e designados em contrato.
5. Contrato de transporte – o objeto deste negócio jurídico não é o navio, mas o "espaço para carga", nesse sentido, há, com relativa frequência, o uso do VCP como contrato de transporte, em função de sua natureza jurídica semelhante.

O conhecimento de embarque (Bill of Lading) um documento costumeiro identificado que remonta ao século XIV ou mesmo antes. O Bill of Lading deve incorporar os termos contratuais previstos no contrato de afretamento, costuma prever situações nas quais a descarga pode ocorrer sem a apresentação do BL. Quanto à responsabilidade. o comandante do navio está sob as ordens do afretador e deve assinar os BL tal como solicitado, não sendo obrigado a assinar BL ilícitos. O afretador deve indenizar o comandante no caso deste ser responsabilizado; assim como o afretador se compromete com o fretador por intermédio de um documento chamado Letter of indemnity(LOI), garante nas hipóteses de responsabilização, assim discriminadas:a primeira, apresentação da LOI sem BL; e,a segunda, se o porto de destino for distinto daquele constante no BL. Até hoje o Bill of Ladind é emitido em papel, em que pesem as reiteradas tentativas de emissão de BL eletrônico. O Bill of Lading é título de crédito, são negociáveis, são dados em garantia e admitem a negociação do objeto ao qual fazem referência (carga). Contudo, o Bill of Lading padece do risco de fraude quanto às assinaturas, problema que foi sanado pelo uso de Blockchain e de assinaturas criptografadas. Todavia, ainda restavam vulnerabilidades quanto ao "double spending"[183].

Ainda há uma carência normativa para o uso de Bill of Lading com base em tecnologia Blockchain.

183 Double Spending é uma falha de sistemas de criptoativos. O Double Spending ocorre se um usuário consegue fazer uso dos mesmos cripto ativos mais de uma vez. Há ferramentas que previnem esse efeito.

Ocorre que na Indústria do Petróleo e Gás, especificamente no segmento midstream podem ocorrer negociações com o óleo cru e desde aquele momento existem Bill of Lading e smart contracts associados a cláusulas condicionando Delivery Orders[184].

Podem ocorrer fraudes relacionadas aos Bill of Lading, como a adulteração e mesmo a falta do documento, o que pode ser suprido com o uso da tecnologia Blockchain, tanto com relação aos smart contracts e assinaturas encriptadas, como pela autenticação. Cláusulas contratuais importantes dos smart contract como, por exemplo, aquelas que tratam dos prazos (PLOMARITOU & PAPADOPOULOS, 2018): Laytime[185], Demurrage[186], e Despatch[187] constam da estrutura blockchain.

Não somente dados de interesse dos contratos, mas a autenticação de registro de embarcações, owners[188], prepostos, gravames (como hipotecas, por exemplo), ou "liability and indemnity marks"[189] presentes na documentação do navio; dados que conferem segurança e agilidade nas transações, e as tornam mais eficientes, com o uso de Blockchain.

Na verdade, nem todas as operações do transporte marítimo se beneficiam significativamente do uso de Blockchain, até porque as fraudes podem ser perpetradas em diversas atividades. As atividades que mais se beneficiam, na opinião do autor, são as seguintes:

1. Quanto ao navio, a checagem de registros, propriedade, delegações para representação (mandatos); verificação de responsabilidade, gravames imputáveis ao navio como hipotecas, arrestos e outros; acesso a contratos e suas cláusulas.
2. Quanto ao Bill of Lading, identificação de propriedade da carga, títulos de crédito, alterações no BL, correções no manifesto de carga.
3. Quanto ao frete, a quitação de pagamentos.
4. Quanto a Demurrage, a quitação e tracking[190].
5. Quanto a Storage[191], pagamento e tracking.
6. Quanto a tripulação, no recrutamento, a identificação e certificação de qualificação.

---

184 Ordens de entrega.

185 Laytime é o tempo de espera, definido como "o período de tempo acordado entre as partes (contratantes) durante o qual o proprietário colocará e manterá a embarcação disponível para carregamento ou descarregamento sem pagamento adicional ao frete".

186 Demurrage é definido como "um valor acordado a pagar ao proprietário em relação ao atraso do navio após o término do tempo de permanência, pelo qual o proprietário não é responsável. A demurrage não estará sujeita às exceções que se aplicam ao tempo de permanência, a menos que especificamente declarado no contrato de fretamento ".

187 Despatch é definido como um valor acordado para ser pago pelo proprietário na hipótese do navio concluir o carregamento ou descarregamento antes do término do tempo de permanência.

188 Owners – termo utilizado para designar o proprietário da embarcação.

189 Liability and Indemnity Marks – Registros de responsabilidade e indenização vinculados ao navio.

190 Tracking, nesse sentido, é rastreamento.

191 Storage é um pagamento sobre o atraso na ocupação de carga seja por desembaraço alfandegário ou por ocupação por tempo demasiado de terminal de contêineres.

7. Quanto aos Agentes de Negociação de Transporte Marítimo, pagamentos e quitações.
8. Quanto às Seguradoras, documentos, prazos, direitos e obrigações, informes.
9. Quanto às entidades de certificação, certificados.
10. Quanto aos Títulos de Crédito e outros papeis, autenticação e identificação de endossados.

No que diga respeito às fraudes envolvendo seguros marítimos, o costume do mar, desde muito tempo, constata a atuação proposital no sentido de provocar "água aberta" [192] para provocar o afundamento do navio; a captura de navios; o desaparecimento de cargas fictícias, ou a simulação da existência de cargas que jamais existiram; a adulteração de cargas; a simulação de roubo de cargas; a simulação de explosão, incêndio supostamente não intencionais. De uma forma sintética, seria a simulação de um acidente da navegação (BRASIL, 1954, Art.14) coberto pelo seguro. A premeditação ocorre antes mesmo da celebração do contrato de seguro. Dispositivos de tracking com base em Blockchain podem reduzir a incidência de fraudes contra o seguro, impactando nos custos.

6.0 Conclusão

O objetivo da pesquisa foi alcançado, na medida em que se logrou descrever a aplicação de tecnologia de proteção de dados na Indústria do Petróleo 4.0.

É inequívoco que os desafios da Indústria do Petróleo e Gás offshore se materializam nas condições de extrema dificuldade operacional, tecnológica e logística. As condições de afastamento das bases a mais de 300 Km, em alto-mar, perfurando em profundidades que alcançam 7000 metros de profundidade, sob condições de pressão, temperatura, sob a influência de correntes marinhas, em camadas geológicas instáveis, com elevado grau de incerteza quanto aos resultados a serem obtidos, e com um custo elevado, em um mercado com variação de preços influenciados por geopolítica, assimetria de informação, altos custos de transação e influência cruzada de outros mercados, somente estas variáveis já seriam suficientes a justificar a pesquisa e desenvolvimento de tecnologias que tivessem por propósito melhorar a eficiência do empreendimento.

A tecnologia Big Data surge como uma demanda natural em função do volume de dados que sensores, em sistemas os mais diversos, produzindo informações nos mais distintos formatos, formando um Data Lake de grande importância na tomada de decisão. O planejamento cíclico, contínuo e flexível, baseado em interpretação de dados, correção de planejamentos, tomada de decisões e ações, precisa de rapidez, precisão e eficiência na implementação.

192 Agua Aberta situação na qual um abertura no costado prejudica a estanqueidade do navio, ameaçando sua estabilidade e podendo levá-lo ao naufrágio.

A gestão de volumes de dados da ordem de milhões de megabytes, com alto grau de heterogeneidade, demanda técnicas de Big Data na Indústria de Petróleo 4.0 pelos muitos motivos que foram detalhadamente apresentados no texto.

A internacionalização da Indústria de Petróleo e Gás, e a complexificação de "Supply Chain Management" onde há a necessidade de fornecimento e abastecimento de itens de empresas de todo o mundo, equipamentos de diversas origens, é outro fatos a justificar o Big Data.

A Indústria do Petróleo e Gás 4.0 integra operational technology, TI e IioT, e somente por esse motivo, o volume de dados que essas tecnologias produzem e precisam ser gerenciados, já justificaria a necessidade de tecnologias de Big Data.

Se não fosse pelos motivos apontados, a arquitetura necessariamente distribuída de dados, e a sensibilidade de protocolos, algoritmos de conformidade, redes inteligentes, e o comportamento de ameaças cada vez mais frequentes e sofisticadas, exigiriam que a Indústria do Petróleo e Gás 4.0 fosse dotada de robusta segurança cibernética, técnicas de encriptação com chaves de alta complexidade e soluções de inteligência artificial e machine learning para se contrapor a hackers e tentativas de ataques cibernéticos cada vez mais elaborados e potentes.

A conectividade e a existência de acessos, a vulnerabilidade que se impõe em um ambiente onde a conectividade e a interoperabilidade acabam por estabelecer larguras de banda elevadas e o volume de dados trafegando em alta velocidade exigem pesquisa e desenvolvimento de técnicas mais eficientes de gerenciamento de Big Data na Indústria de Petróleo 4.0. Contudo, o que maior motivo a justificar o desenvolvimento de uma regulação específica de proteção de dados, sejam por aspectos de dados de propriedade Indústrial, sejam por questões estratégicas, é o desenvolvimento baseado em capacidades de Data Analytics.

Quanto ao uso da tecnologia de Blockchain na Indústria de Petróleo e Gás 4.0, pode-se concluir que as questões de segurança são a maiores justificativas, sejam por lidar com criptoativos que carecem de legislação nacional a tratar com um mercado que já está em operação; seja pelas necessidades de segurança de dados, já mencionada; seja pela segurança de smart contracts, tendência irreversível e que no segmento downstream avulta de importância por conta das fraudes, que há muito ocorrem, ressalte-se, e particularmente quanto ao navio, ao Bill of Lading, ao frete, ao Demurrage, ao Storage, à tripulação, aos Agentes de Negociação de Transporte Marítimo, ao Seguro, às entidades de certificação, e às negociações com Títulos de Crédito e outros papeis transacionados no transporte marítimo. Blockchain representa segurança contratual, agilidade, um incremento nos negócios e um problema para os Estados no que tange à tributação. Há que se ressaltar que as demais fraudes no downstream são severamente restritas pela capacidade de rastreamento e certificação.

A realidade da Indústria de Petróleo e Gás 4.0 representa um desafio jurídico, além de um enorme esforço de pesquisa e desenvolvimento, As tecnologias trazem ao direito novas oportunidades e novos problemas, interesses e assimetrias, a colocar o Estado e as empresas em situação de expectativa, pois as consequências da entrada inevitável dessas tecnologias provocará uma mudança radical nos institutos até então firmemente estabelecidos. Emerge o Direito da Tecnologia como ramo autônomo e com sua hermenêutica própria, onde os princípios e valores são desafiados por funcionalidades até então desconhecidas, como a capacidade de transações diretas entre particulares e de intervenção estatal impossível, esse é apenas um exemplo do que se denomina tecnologia disruptiva.

REFERÊNCIAS

AHMED, S.; KHAN, R.H.. **Blockchain and Industry 4.0.** In. Blockchain in Data Analytics. Mohiuddin Ahmed (Editor). Newcastle upon Tyne: Cambridge Scholars Publishing, 2020.

ALAM, M.; SHAKIL, K.A.; KHAN, S.. **Internet of Things (IoT)**: Concepts and Applications. Switzerland: Springer Nature Switzerland AG, 2020.

ALLIANZ. **Allianz Risk Barometer**: Identifying the major business risks for 2020. Disponível em: < https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2020.pdf >. Acesso em 04 de dezembro de 2020.

ANP. Agência Nacional do Petróleo, Gás Natural e Biocombustíveis. **Consulta e Audiência Públicas nº 16/2020**. Disponível em < http://www.anp.gov.br/consultas-audiencias-publicas/concluidas/5997-consulta-audiencia-publica-n-16-2020 > Acesso em 14 de novembro de 2020.

BRASIL. Lei nº 7.652, de 3 de fevereiro de 1988. **Dispõe sobre o registro da Propriedade Marítima**. Disponível em: < http://www.planalto.gov.br/Ccivil_03/Leis/L7652.htm >. Acesso em 5 de dezembro de 2020.

BRASIL. Lei nº 2.180, de 5 de fevereiro de 1954. **Dispõe sobre o Tribunal Marítimo**. Disponível em: < http://www.planalto.gov.br/ccivil_03/LEIS/L2180compilado.htm >.Acesso em: e de dezembro de 2020.

BRASIL. MARINHA. DPC. Diretoria de Portos e Costas. NORMAM. Normas da Autoridade Marítima. NORMAM-13 - Normas da Autoridade Marítima para Aquaviários. 2003. Disponível em: < http://sites.mplopes.com.br/dpcnovo/sites/default/files/normas/normam13.pdf >. Acesso em 5 de dezembro de 2020.

BRASIL. Lei nº 9.537, de 11 de dezembro de 1997. **Dispõe sobre a segurança do tráfego aquaviário em águas sob jurisdição nacional**. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l9537.htm >. Acesso em 5 de dezembro de 2020.

BRASIL. Lei nº 9.478, de 6 de agosto de 1997. **Dispõe sobre a política energética nacional, as atividades relativas ao monopólio do petróleo, institui o Conselho Nacional de Política Energética e a Agência Nacional do Petróleo e dá outras providências**. Publicada no Diário Oficial da União de 7 de agosto de 1997. Disponível em: < https://www.planalto.gov.br/ccivil_03/leis/l9478.htm > Acesso em 14 de novembro de 2020.

BRASIL. ANP - Agência Nacional do Petróleo, Gás Natural e Biocombustíveis. Ministério de Minas e Energia. Resolução nº 810, de 16 de março de 2020. **Institui a gestão de segurança operacional de terminais para movimentação e armazenamento de petróleo, derivados, gás natural e biocombustíveis nos termos do Regulamento Técnico de Terminais para Movimentação e Armazenamento de Petróleo, Derivados, Gás Natural e Biocombustíveis** – RTT. Publicado no Diário Oficial da União. Publicado em: 17/03/2020. Edição: 52. Seção: 1. Página: 53.

CASTRO JR, O. A.. **Introdução ao Direito Marítimo**. In. Temas Atuais de Direito do Comércio Internacional. Osvaldo Agripino de Castro Jr. vol. I. Florianópolis: Editora da OAB/SC, 2004.

CISO ADVISOR. **Cibercriminoso anuncia venda de acesso a redes da ANP e Petrobrás.** Disponível em < https://www.cisoadvisor.com.br/cibercriminoso-alega-ter-acesso-a-redes-da-anp-e-petrobras/ >. Acesso em 24 de novembro de 2020.

CISO ADVISOR. **Ataques ao setor de petróleo e gás aumentam 38% no primeiro semestre**. Disponível em: < https://www.cisoadvisor.com.br/ataques-ao-setor-de-petroleo-e-gas-aumentam-38-no-primeiro-semestre/ >. Acesso em 05 de dezembro de 2020.

KPMG. A **KPMG** é uma rede global de firmas independentes que prestam serviços profissionais de Audit, Tax e Advisory. Disponível em: < https://home.kpmg/br/pt/home/Indústrias/energia-recursos-naturais/petroleo-gas.html >. Acesso em 05 de dezembro de 2020.

LU,H.; HUANG, K.; AZIMI, M.; and GUO, L.. **Blockchain Technology in the Oil and Gas Industry**: A Review of Applications, Opportunities, Challenges, and Risks. IEEE Access Multidisciplinary Open Access Journal.IEE Access Journal. April 11, 2019.

MOHANTA, B.; NANDA, P.; PATNAIK, S.. **Management of V.U.C.A. (Volatility, Uncertainty, Complexity and Ambiguity) Using Machine Learning Techniques in Industry 4.0 Paradigm**. In. New Paradigm of Industry 4.0: Internet of Things, Big Data & Cyber Physical Systems. Srikanta Patnaik (editor). Switzerland: Springer Nature Switzerland AG. 2020.

PLOMARITOU, E.; PAPADOPOULOS, A.. **Shipbroking and Chartering Practice**. 8 ed. Oxford: Informa Law from Routledge, 2018.

QUINTANS, Luiz Cezar P. **Manual de direito do petróleo**. São Paulo: Atlas, 2015.

SALO, k.; ZETTERDAHL, M.; JOHNSON, H.; SVENSSON, E.; MAGNUSSON, M.; GABRIELII, C; BRYNOLF, S.. **Emissions to the Air**. In. Shipping and the Environment Improving Environmental Performance in Marine Transportation. Karin Andersson; Selma Brynolf; J. Fredrik Lindgren; Magda Wilewska-Bien (Editors). Berlin: Springer-Verlag Berlin Heidelberg, 2016.

SINGH, M.. **Blockchain Technology for Data Management in Industry 4.0**. In. Blockchain Technology for Industry 4.0: Secure, Decentralized, Distributed and Trusted Industry Environment. Rodrigo da Rosa Righi, Antonio Marcos Alberti, Madhusudan Singh (Editors). Singapore: Springer Nature Singapore Pte Ltd., 2020.

SOYER, B. **Marine Insurance Fraud**. Oxford: Informa Law from Routledge, 2014.

SURESH, A; NANDAGOPAL, M.; RAJ, P.; NEEBA, E. A.; LIN, J.W.. **Indústrial IoT Application Architectures and Use Cases**. Boca Raton: Taylor & Francis Group, 2020.

TOMA, C.; POPA, M. **IoT Security Approaches in Oil & Gas Solution Industry 4.0**. Informatica Economica Journal. vol. 22. nº. 3 Romania: INFOREC Association, 2018.

NGUYEN, T.; GOSINE, R.G.; WARRIAN, P.. **A Systematic Review of Big Data Analytics for Oil and Gas Industry 4.0**. IEEE Access is a multidisciplinary, open access journal of the IEEE. Received February 13, 2020, accepted March 3, 2020, date of publication March 9, 2020, date of current version April 10, 2020. Volume 8, 2020. pp. 61183 – 61201.

TYAGI, H.; KUMAR, R. **Cloud Computing for IoT**. In. Internet of Things (IoT): Concepts and Applications. Mansaf Alam; Kashish Ara Shakil; and, Samiya Khan(Editors). Switzerland: Springer Nature Switzerland AG, 2020.

SOCIEDADE DA INFORMAÇÃO E VIGILÂNCIA

Marcella da Costa Moreira de Paiva
Paula Cristiane Pinto Ramada
Telson Pires

INTRODUÇÃO

A evolução das tecnologias de informação e de comunicação, à luz do capitalismo e industrialismo, sustenta a formação da sociedade de informação, que se estrutura por meio do gerenciamento e do processamento de informações. Isto provoca novas preocupações na modernidade, como a proteção de dados pessoais.

A modernidade já se possuía o binome vigilância privacidade, já que se baseia na proteção de direitos de primeira geração e limitação do estado. Contudo, o surgimento da internet expande a preocupação com o controle para outros atores, as empresas de tecnologia, assim como depende do fortalecimento da salvaguarda dos dados pessoais.

O presente texto tem como objetivo a análise do cenário da sociedade da informação, à luz da dualidade entre vigilância e proteção de dados pessoais. Para tanto, parte-se da contextualização da sociedade da informação e o seu impacto nos direitos fundamentais, em especial, na privacidade e tutela de dados pessoais. Posteriormente, trata-se das consequências da excessiva vigilância. Neste passo, propõe-se a cidadania digital como alternativa, sendo um ponto de convergência entre o informacionalismo e a privacidade.

1. A SOCIEDADE DE INFORMAÇÃO E SEUS IMPACTOS

A revolução tecnológica centralizada no desenvolvimento da informação introduziu uma nova interpretação a estrutura material a sociedade sob uma celeridade descontrolada. Com isto, a noção da sociedade da informação[193] tomou forma na esteira da invenção de máquinas de inteligência artificial durante a segunda guerra da mundial, momento em que a informação assumiu um papel primordial na sociedade ganhando *status* de fenômeno social[194].

193 A sociedade da informação é um conceito sociológico pormenorizado por Manuel Castells, sendo um fenômeno paradigmático de transformação social e econômica. CASTELLS, Manuel. **A Sociedade em Rede**: a era de informação: economia, sociedade e cultura. Trad.: Roneide Venancio Majer. 17ed., São Paulo: Paz e Terra, 2016, p. 108-109.

194 Sugiro a leitura da Obra "IBM e o Holocausto" que retrata a empresa IBM criada pelo alemão Herman Hollerith, uma das maiores potências em tecnologia, foi criada com finalidade de contar pessoas de uma forma inédita com o recurso de identificar e quantificar. A tecnologia da IBM demonstrou que era capaz de fazer maior de que apenas contar pessoas e coisas, possuindo tecnologia de registrar dados, processa-los, recupera-los, analisa-los e automaticamente responder perguntas específicas. Tal empresa, motivada pela ganância e pelo lucro, sem

Entretanto, foi na Califórnia, Estados Unidos da América, na década de 70 do século XX, na região atualmente conhecida como Vale do Silício, que iniciou esse novo segmento tecnológico com relação à economia e à geopolítica, materializando uma nova forma de produção, comunicação, administração e vida, impactando as formas e evolução das novas tecnologias de informação em que se difundiram amplamente, acelerando seu desenvolvimento sinérgico e o convergindo em um novo paradigma[195].

A internet foi partejada pelos especialistas tecnológicos da Agência de Projetos de pesquisa avançada do Departamento de Defesa dos Estados Unidos com a finalidade de inibir a tomada ou a perda do sistema americano de comunicações pelos soviéticos em caso de guerra nuclear. Tal invenção tornou a base de uma rede de comunicação horizontal global compostas de milhares de rede de computadores adequada por pessoas e grupos no mundo todo e com inúmeras formas de objetivos[196].

Todavia, foi no final do século XX, o verdadeiro cerne da revolução da tecnologia[197] da informação, que concretizou a transformação da cultura material entrelaçada em torno da tecnologia da informação por meio de novos mecanismos tecnológicos que trouxeram grandes avanços positivos no campo na energia, medicina e transporte[198].

Importante salientar que a revolução tecnológica não extinguiu a relevância do trabalho e dos recursos materiais para economia, mas inaugurou uma fonte nova de produção de riqueza e diminuição dos custos concretizado na administração das informações. Manuel Castells estabelece tecnologia como "o uso de conhecimentos científicos para especificar as vias de se fazerem as coisas de maneira reproduzível". Leciona ainda que tecnologia da informação é o "conjunto convergente de tecnologias em microeletrônica, computação e

---

levar em conta as implicações morais, colocou a tecnologia de cartões perfurados à disposição dos nazistas. BLACK, Edwin. **A Aliança Estratégica entre a Alemanha Nazista e a mais poderosa empresa Americana**

195A microeletrônica causou uma revolução dentro da revolução. CASTELLS, Manuel. **A Sociedade em Rede**: a era de informação: economia, sociedade e cultura. Trad.: Roneide Venancio Majer. 17ed., São Paulo: Paz e Terra, 2016., p. 64-65.

196 CASTELLS, Manuel. **A Sociedade em Rede**: a era de informação: economia, sociedade e cultura. Trad.: Roneide Venancio Majer. 17ed., São Paulo: Paz e Terra, 2016., p.65-66.

197 A cada dia que passa a tecnologia vem avançado com surgimento de processadores de informações mais potentes e mais rápidos, além das transmissões dos dados que podem ser feitas por todas as vias imagináveis. Nesse sentido, cita a Lei de Gordon Moore que constatou que a cada um ano e meio a capacidade de processamento dos computadores dobra, ou seja, a cada 18 meses inovam as técnicas de informações. Isso significa que em 2025 um computador será 64 vezes mais rápido do que é em 2014. Outra lei, fincada no campo de transmissão de informação, afirma que a quantidade de dados transmitidos por cabos de fibra ótica, a forma mais veloz de conectividade de dados, dobra a cada nove meses aproximadamente.

198 CASTELLS, Manuel. **A Sociedade em Rede**: a era de informação: economia, sociedade e cultura. Trad.: Roneide Venancio Majer. 17ed., São Paulo: Paz e Terra, 2016., p.67-70.

telecomunicações/radiodifusão, e optoeletrônica" bem como "a engenharia genética e seu crescente conjunto de desenvolvimentos e aplicações"[199].

O método atual de mudança tecnológica amplia-se extremamente em consequência de sua capacidade de criar dispositivo para a troca de informação entre ramos tecnológicos por meio de uma linguagem digital comum na qual a informação é gerada, armazenada, recuperada, processada e transmitida[200].

Dessa forma, Pierre Lèvy, argumentando sobre o dilúvio das informações por conta da natureza exponencial, explosiva e caótica do crescimento das telecomunicações, assevera que

> "(...) a quantidade bruta de dados disponíveis se multiplica e se acelera. A densidade dos links entre informações aumenta vertiginosamente nos bancos de dados, nos hipertextos e nas redes. Os contratos transversais entre os indivíduos proliferam de forma anárquica. É o transbordamento caótico das informações, a inundação de dados, águas tumultuosas e os turbilhões de comunicação, a cacofonia e o psitacismo ensurdecedor das mídias" [201].

Por sua vez, Manuel Castells leciona que:

> "(...) o que caracteriza a atual revolução tecnológica não é centralizada de conhecimentos e informação, mas aplicação desses conhecimentos e dessa informação para geração de conhecimentos e de dispositivos de processamento/comunicação da informação, em um ciclo de realimentação cumulativo entre inovação e seu uso"[202].

Nesse sentido, o avanço da circulação de informação no mundo atual fundamenta a assertiva de que vivemos hoje em uma sociedade de informação. A sociedade de informação, como requisito qualificador do momento atual da experiência humana, o fazemos admitindo que podemos caracterizar o modo de desenvolvimento atual como baseado na informação, assumindo-o como núcleo de importantes transformações na esfera econômica, política e cultural.

Nesse contexto, vivemos em uma sociedade em que a informação ocupa um lugar fundamental, fruto de uma radical urbanização da sociedade, iniciada na revolução Industrial e se intensifica no século XX, por motivos de critérios econômicos e políticos.

A importância da informação potencializou a partir do desenvolvimento vertiginoso da informática, entendida como tratamento automático da informação. O impacto desse potencial de plataformas tecnológicas e seu poder inerente privam os cidadãos do poder de controlar suas

---

199 CASTELLS, Manuel. **A Sociedade em Rede**: a era de informação: economia, sociedade e cultura. Trad.: Roneide Venancio Majer. 17ed., São Paulo: Paz e Terra, 2016., p. 87.
200 NEGROPONTE, Nicholas. **A vida digital**. Tradução: Sérgio Tellaroli. São Paulo: Companhia das Letras, 1995.
201 LÉVY, Pierre**. Cibercultura**. Rio de Janeiro: Editora 34, 2000, p. 13.
202 CASTELLS, Manuel. **A Sociedade em Rede**: a era de informação: economia, sociedade e cultura. Trad.: Roneide Venancio Majer. 17ed., São Paulo: Paz e Terra, 2016, p. 87.

informações pessoais na esfera virtual, o que gerará consequências. O desafio maior é tentar recuperar um controle de privacidade por meio da autodeterminação informativa, ou seja, o titular dos dados deve ter o direito de ser informado pelo uso dos seus dados, com a finalidade da imputação do consentimento.

Dessa forma, com o progresso tecnológico a vulnerabilidade da privacidade se evidenciou, refletindo na vida cotidiana do cidadão, uma vez que a vigilância dos membros na sociedade vem recrudescendo, silenciosa e diuturnamente há muitas décadas, caracterizando-se mesmo como um atributo do mundo contemporâneo[203].

A título de exemplo, cita-se o Google[204], que constantemente vigia os seus usuários. *Verbi gratia*, em um vídeo disponível no site do *You Tube*, um carro de venda de sorvetes, denominado Google, convoca crianças para os experimentar os sorvetes, porém, quando as crianças vão ser atendidas, o motorista se nega a entregar o sorvete, ironizando que "deveriam saber que não há soverte grátis" e, enquanto, as crianças recebem o sorvete grátis, são scaneados. Outro exemplo são os aplicativos de celulares, que constantemente solicitam a localização do usuário. As empresas vigiam tanto os seus clientes que conseguem, por meio de suas compras, saberem quando estão grávidas ou não, se são solteiros, casados, separados ou divorciados.

Existem inúmeras técnicas para a coleta de dados sobre a pessoa com a finalidade da materialização de publicidade comportamental. A presença de pessoas, hoje, em redes sociais é um fator que favorece a obtenção de dados e a concretização de perfis. Danah Boyd e Nicole Ellison afirmam

> "(...) como principais características das redes sociais a construção de um perfil público ou semipúblico dentro de um determinado sistema; a articulação de uma lista de outros usuários deste sistema com os quais se quer estabelecer um relacionamento;

---

203 [ ] Kaminsk esclarece que "a tecnologia não é neutra. É a junção entre ciência, mercado e sociedade. Mas a tecnologia, por si só, não viola a privacidade, e sim as pessoas que utilizam dessa tecnologia, criada para suprir necessidades, e a política por detrás da tecnologia. Pode ser usada para invadir a privacidade, e pode ser usada para protege-la. Em suma, a tecnologia deve garantir aos indivíduos o direito à privacidade na internet. E a privacidade das informações deve ser valorizada por todos aqueles que valorizam a liberdade. Devemos mudar nossa forma de pensar, nossas leis e nossa sociedade. Devemos criar um futuro que preze a liberdade, e que honre a autonomia e a privacidade pessoal. E devemos começar agora". KAMINSKI, Omar. Privacidade na Internet. *In: R*OVER, Aires José. **Direito, sociedade e informática: Limites e perspectivas da vida digital.** Florianópolis: Fundação Boiteux, p. 94-103, 2000, p.100-101.

204 Em 1998, Larry Page e Sergey Brin, estudantes da Universidade de Stanford, criaram a ferramenta de busca, google, com o diferencial de inexistência de anúncios e fontes de receitas, porém, em 2000, passou a exibir publicidades e, em 2004, terminou por adquirir as empresas Where2 e keyhole, originando a google maps. Mais tarde, nos anos 2006 e 2008 incorporou-se o youtube e a Doubleclick. Em 2010, o jornal Wall street realizou a teses que revelaram que alguns sites dos Estados Unidos instalavam cookies nos computadores dos visitantes, com finalidade de monitorar os hábitos de navegação daqueles que acessavam. Disponível: [http://online.wsj.com/public/page/what-they-know-digital-privacy. Acesso em: 15 set. 2019.

> e a visualização de navegação pela sua lista de conexões e pela aquela de outros através do sistema"[205].

Ilse Aigner, quando Ministra alemã de Defesa do Consumidor em 2010, afiançou, sobre os sites visitados na internet, que "as pessoas devem ter consciência de que se trata de um modelo de negócio. O serviço oferecido não é gratuito. Nós, usuários, pagamos por este serviço com as nossas informações privadas"[206]. Emilie Barrau, comenta que tal "sistema beneficia o comércio e a publicidade na internet, pois quanto mais as pessoas tiverem acesso aos dados de usuários, melhor e mais específica pode ser a publicidade direcionada a estes usuários" [207]. Barrau afirma ainda, "se as condições de uso não forem lidas, e a maioria dos usuários não o faz porque não as entendem, então não se sabe com o que se está concordando. Quando se quer lê-las precisa-se de 30 minutos a uma hora. Tornando-se um pesadelo as condições de uso e privacidade" [208].

Neste contexto, podemos afirmar que os serviços disponíveis em rede obrigam a coleta, o armazenamento e o tratamento de dados, que podem revelar os hábitos de consumo, as opiniões políticas, a localização e as preferências dos seus usuários. Assim, cita Castells:

> "O aspecto mais atemorizante é, de fato, a ausência de regras explícitas de comportamento, de previsibilidade das consequências de nosso comportamento exposto, segundo os contextos de interpretação, e de acordo com critérios usados para julgar nosso comportamento por uma variedade de atores atrás da tela de nossa casa de vidro. Não é o Big Brother, mas uma multidão de irmãzinhas, agências de vigilância e processamento de informações que registram nosso comportamento para sempre, enquanto bancos de dados nos rodeiam ao longo da nossa vida - a começar, dentro em breve, com nosso DNA e características pessoais (nossa retina, nosso datilograma, na forma de marcas digitalizadas). Nas condições vigentes nos Estados autoritários, essa vigilância pode afetar diretamente nossas vidas (essa é de fato a situação da maioria esmagadora da humanidade). Mas mesmo em sociedades democráticas, em que os direitos civis são respeitados, a transparência de nossas vidas moldará decisivamente as nossas atitudes. Ninguém jamais foi capaz de viver numa sociedade transparente. Se esse sistema de vigilância e controle da Internet se desenvolver plenamente, não poderemos fazer o que nos agrada. Talvez não tenhamos nenhuma liberdade e nenhum lugar onde nos esconder "[209].

---

205 BOYD, Danah; ELLISON, Nicole. **Social network sites**: definition, history, and scholarship. 2007. Disponível em :<www.guilford.edu/about_guilford/services_and_administration/library/libguide_images/boyd.pdf>. Acesso em 12.12.2018.

206 Perigos na rede são temas no Dia da Segurança na internet. 09.02.2010. Disponível em https://www.dw.com/pt-br/perigos-na-rede-s%C3%A3o-tema-no-dia-da-seguran%C3%A7a-na-internet /a-5233581. Acesso em 12.12.2018. Em pesquisa realizada pela Bitkom e pelo instituto Forsa, cerda de 6% dos usuários em todo o mundo são membros de comunidades virtuais.

207 Perigos na rede são temas no Dia da Segurança na internet. 09.02.2010. Disponível em https://www.dw.com/pt-br/perigos-na-rede-s%C3%A3o-tema-no-dia-da-seguran%C3%A7a-na-internet /a-5233581. Acesso em 12.12.2018. Em pesquisa realizada pela Bitkom e pelo instituto Forsa, cerda de 6% dos usuários em todo o mundo são membros de comunidades virtuais.

208 Perigos na rede são temas no Dia da Segurança na internet. 09.02.2010. Disponível em https://www.dw.com/pt-br/perigos-na-rede-s%C3%A3o-tema-no-dia-da-seguran%C3%A7a-na-internet /a-5233581. Acesso em 12.12.2018. Em pesquisa realizada pela Bitkom e pelo instituto Forsa, cerda de 6% dos usuários em todo o mundo são membros de comunidades virtuais.

209 CASTELLS, Manuel. **A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade.** Tradução de Maria Luiza X. de A. Borges, Revisão de Paula Vaz. Rio de Janeiro: Jorge Zahar, 2003, p. 148-149.

Por conseguinte, não há como negar que a intensa vigilância na sociedade de informação potencializou a insegurança e a ameaça aos inúmeros Direitos Fundamentais.

2. DIREITO À PRIVACIDADE

Todos os seres humanos possuem direitos inalienáveis e relevante em razão do seu objeto que se manifesta como algo fundamental, e assim, são tratados como bens de maior valor jurídico[210]. Desses direitos essenciais, cita-se o direito da privacidade, pois remetem a valores numa disposição hierárquica como fundamentais de todo ser humano, capacitado a impor respeito perante o Estado e perante aos outros seres humanos, do mesmo modo, o Estado deve protegê-la, uma vez que sua proteção trata de modalidade de tutela da dignidade da pessoa humana[211].

A Constituição Federal de 1988 tutela o direito à privacidade, ampliando, a proteção dos dados pessoais como um direito fundamental, que, felizmente, em 2019 foi confeccionada a PEC 17, inserindo no rol dos direitos garantias e fundamentais, no artigo 5º, XII da CF, "o direito a proteção de dados pessoais, inclusive no meio digital". Embora, "inter-relacionados, o conceito de privacidade não se confunde com o conceito de dados pessoais", como comenta Eduardo Magrani[212], ao citar Stefano Rodotà e Danilo Doneda como base jurídica para distinção dos institutos.

Para o jurista italiano, a privacidade está baseada como no "direito de controlar suas próprias informações e de determinar a maneira de construir sua própria esfera particular"[213], diferente do conceito de dados pessoais, que "é a maneira indireta de atingir um objetivo último, que é a proteção da pessoa", ou seja, "os dados pessoais representam algum atributo de uma pessoa identificada ou identificável e, portanto mantêm uma ligação concreta e viva com a pessoa titular destes dados", visto que "os dados pessoais são a pessoa e como tal devem ser tratados, justificando o recurso ao instrumental jurídico destinado à tutela da pessoa"[214].

---

210 DE CUPIS, Adriano. **Direitos da Personalidade**. Trad.: REZENDE, Afonso Celso Furtado. Campinas: Romana, 2004, p. 29.
211 ASCENSÃO, José Oliveira. **Direito Civil: teoria geral**. 2 ed. Coimbra: Coimbra, 2000, p. 40.
212 MAGRANI, Eduardo. **Entre dados e robôs: ética e privacidade na era da hiperconectividade**. 2 ed. Porto Alegre: Arquipelágo, 2019, p. 56.
213 RODOTÁ, Stefano. **A vida na Sociedade de Vigilância. A privacidade hoje.** Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Doneda. Rio de Janeiro: Renovar, 2008, p. .....
214 BRASIL. Escola Nacional de Defesa do Consumidor. *A* **proteção de dados pessoais nas relações de consumo: para além da informação creditícia**. Elaboração Danilo Doneda. Brasília:SDE/DPDC, 2010, p. 39.

Tal distinção, é verificada na Carta dos Direitos Fundamentais da União Europeia e o Tratado que estabelece uma Constituição para a Europa quando reconhecem a privacidade e a proteção de dados pessoais como um direito autônomo, diz Rodotà[215]. Menciona ainda, que a diferença, "não é fachada: no direito ao respeito à vida privada e familiar manifesta-se, sobretudo, o momento individualista e o poder exaurem substancialmente na exclusão da interferência de outrem; a tutela, portanto, é estática e negativa"[216]. Ao contrário da "proteção de dados pessoais que fixa as regras sobre a modalidade de tratamento dos dados e concretiza-se em poderes de intervenção; a tutela é dinâmica, segue os dados em sua circulação". [217]

Nesse sentido, mesmo com distinções em seus conceitos, ao tutelar o direito à privacidade não como concessão que o Direito faz à pessoa, mas como reconhecimento da individualidade do ser humano, assim como a proteção dos dados pessoais. O que se protege é a pessoa, logo o descumprimento dos direitos e garantias fundamentais conduz a indenização.

O direito à privacidade [218] representa uma conquista relativamente recente, sendo primeiramente discutido nos direitos de primeira geração[219], buscando a proteção do particular contra intromissões estatais injustas[220].

O início da evolução doutrinária sobre o direito à privacidade ocorreu como consequência da utilização de novas tecnologias na sociedade de informação, que passaram a possibilitar o acesso e divulgação de dados relativos à esfera privada do indivíduo de um modo não pensado no passado.

---

215 RODOTÀ, Stefano***. Tra diritti fondamentali ed elasticità della normativa: il nuovo códice sulla privacy.*** Disponível em http://www.litis.it. Acesso em 27 jan. 2020.

216 RODOTÀ, Stefano. **Tra diritti fondamentali ed elasticità della normativa: il nuovo códice sulla privacy**. Disponível em http://www.litis.it. Acesso em 27 jan. 2020.

217 RODOTÀ, Stefano. **Tra diritti fondamentali ed elasticità della normativa: il nuovo códice sulla privacy**. Disponível em http://www.litis.it. Acesso em 27 jan. 2020.

218 [ ] Macel Leonardi relata que alguns doutrinadores, ensinam que a palavra privacidade é derivada da língua inglesa *privacy*, tendo como expressão exata a palavra privacidade, que vem de privativo e, não privacidade, que seria erroneamente utilizado. Entretanto, outros autores ensinam que a crítica não tem fundamento, dizendo que a palavra *privacy* tem origem no latim, decorrente de *privare*, com a forma adjetiva *privatus* e a expressão privacidade é usada pela Constituição portuguesa LEONARDI, Marcel. **Tutela e Privacidade na Internet**. São Paulo: Saraiva, 2012, p. 45.

219 [ ] Norberto Bobbio preleciona que o direito de primeira geração são os direitos históricos caracterizados por luta em defesa de novas liberdades contra velhos poderes, e nascido de forma gradual, não todos de uma vez e nem de uma vez por todas. BOBBIO, Norberto. **A Era dos Direitos**. Trad.: COUTINHO, Carlos Nelson. Rio de Janeiro: Elsevier, 2004, p.25.

220 AZEVEDO, Fábio. Privacidade e Tratamento dos Dados Pessoais. *In:* MARTINS, Guilherme Magalhães (Coord.). **Temas de Responsabilidade Civil.** Rio de Janeiro: Lúmen Juris, 2011, p.342.

A doutrina atribuiu como marco inicial do direito à privacidade o artigo *The right to privacy*[221], publicado em 1890 na *Harvard Law Review*[222]. Escrito por Samuel Warren e Louis Brandeis, o texto comenta da necessidade de identificar a privacidade na *common law*, a partir de precedentes jurisprudenciais de tribunais ingleses[223], além da proteção total da pessoa e da propriedade, bem como da necessidade de em tempos em tempos definir, novamente, a exata natureza e a extensão de tal proteção contra intromissões indesejadas na esfera pessoal[224].

Foi a partir do indigitado artigo *The rigth to privacy* que a proteção à privacidade, marcada por um individualismo exacerbado e mesmo egoísta, moldou a feição do direito de ser deixado só (*the rigth to be let alone)*. Esse período remonta ao paradigma da privacidade com uma *zero-relationship*, como a ausência de comunicação entre o sujeito e os demais.

Tal noção da privacidade, como direito a ser deixado só, influenciou não apenas a doutrina e a jurisprudência norte americana, como também a de outros países, de forma que encontramos autores sustentando que o respeito à vida privada se traduz em um dever de abstenção (não fazer) [225].

Neste sentido, pondera Doneda:

> "A tutela da privacidade como "direito a ser deixado só", associada ao isolamento, à redução, não nos permite determinar parâmetros para julgar o que ela representa em um mundo no qual o fluxo de informações aumenta incessantemente, assim como aumenta o número de oportunidades de realizarmos escolhas que podem influir na definição da no esfera privada'[226].

No transcorrer do século XX, a mudança da função do Estado, aliada ao progresso tecnológico, colaborou para alterar o sentido e o alcance do direito à privacidade. De um direito com uma dimensão estritamente negativa e com uma acepção quase egoísta, passou a ser considerado como uma garantia de controle do indivíduo de suas próprias informações e como pressuposto para qualquer regime democrático[227].

---

221 Todos os estudiosos não deixam de fazer referência a esse artigo, devido ao pioneirismo empregado para a estruturação científica do direito à privacidade.

222 Era o fim do século XIX, marcado por um período repleto de conquistas individuais vitoriosas e individualista burguesia, que desejava isolamento e tranquilidade.

223 MENDES, Laura Schertel. O direito Fundamental à Proteção de Dados Pessoais. **Revista de Direito do Consumidor**, São Paulo, a. 20, v. 79, p. 45-82, 2011, p. 48.

224 O artigo discute sobre a divulgação não autorizada e indesejada, por um jornal de Boston, de uma lista de convidados e de detalhes do casamento da filha do Senador Samuel D. Warren. De acordo com a tese de Samuel Warren e Louis Brandeis, os envolvidos no evento seriam titulares do direito à privacidade, assim entendido *o direito a ser deixado só*, embora a conclusão levasse em consideração outros interessados violados, como o direito à propriedade.

225 LEONARDI. *Tutela* ..., cit., p. 54.

226 DONEDA. *Da privacidade*...,cit., p.1.

227 [ ] Neste sentido, Rodatà afirma que o século passado vivenciou um processo de inexorável reinvindicação da privacidade. RODOTÀ, Stefano. A **vida na sociedade de vigilância:** a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 15.

O Direito à privacidade modificou-se qualitativamente à medida que sugiram novos desafios ao ordenamento jurídico, a partir do tratamento informatizados dos dados para fazer emergir a dimensão da proteção dos dados pessoais.

Foi a partir de 1960 que esse cenário começa a se alterar. O desenvolvimento tecnológico e a consequência multiplicação de mecanismos para a coleta, armazenamento, processamento, utilização da informação, decorrente da massificação das relações contratuais, estimularam um crescimento significativo do fluxo de dados na sociedade contemporânea. Tais informações passam a ser utilizadas no tráfego social para finalidades diversas[228].

Essa transformação do conceito de direito da privacidade é verificada de forma mais clara a partir da década de 70 do século XX, como por exemplo, nos Estados Unidos da América que, somente por ocasião dos censos realizados nos anos de 1790-1840, o problema da privacidade das informações apareceu somente em relação aos dados relacionados à atividade econômica.

Em Portugal, a proteção de dados pessoais obteve importância constitucional com o artigo 35 da Constituição Portuguesa de 1974, estabelecendo que "todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, no termos da lei"[229]. Assim como na Constituição da Espanha de 1978, que estabeleceu que "a lei limita o uso da tecnologia da informação para garantir a honra e a intimidade pessoal e familiar dos cidadãos e o pleno exercício dos seus direitos"[230].

Na evolução do conceito de privacidade, a decisão do Tribunal Constitucional Alemão no julgamento da Lei do Censo de 25 de março de 1982 é considerada um marco histórico. A Decisão criou o marco para a proteção de dados pessoais e para futuras normas nacionais ou europeias sobre o tema, ao reconhecer um direito subjetivo fundamental e erigir o indivíduo como protagonista no processo de tratamento de seus dados[231].

Após a lei do Recenseamento de População, Profissão, Moradia e Trabalho, que iniciou a ideia de privacidade como proteção de dados pessoais, que determinava o recenseamento geral da população, coletando-se dados relativos ao domicílio, profissão e renda dos indivíduos, com objetivo de reunir informações estatísticas, como crescimento populacional, densidade

228 SCHREIBER, Anderson. **Direito da Personalidade**. São Paulo: Atlas, 2011, p. 129.
229 PORTUGAL, **Constituição da República Portuguesa de 1974**. Disponível em <http://www.fd .uc.pt/CI/CEE/OI/Constituição_Portuguesa.htm>. Acesso em 16 jun. 2018.
230 ESPANHA, **Constitución Española de 1978**. Disponível em <http://www.congreso.es/consti/constitucion/indice/articulos.jsp?ini=15&fin=29&tipo=2>. Acesso em 16 jun. 2018.
231 MENDES. O direito..., *cit.*, p.51-52.

demográfica e atividades econômicas; além de compará-las com dados armazenados em registros públicos e enviá-las a instituições públicas, quando necessárias.

A Corte alemã declarou que o moderno processamento de dados pessoais constitui uma grave ameaça à personalidade do indivíduo, na medida em que permite o armazenamento ilimitado de dados, assim como possibilita a sua combinação de modo a formar um retrato completo da pessoa, sem a sua participação ou conhecimento.

Nesse sentido, afirmar-se que a associação entre o direito à privacidade e os dados pessoais é proporcionado através do progresso tecnológico na sociedade de informação, pois permite o armazenamento e processamento dos dados de forma rápida e eficaz.

Nesse contexto, observa-se que, com a globalização tecnológica, surgem novos problemas e desafios no ordenamento jurídico, pois tais mudanças vieram alterar não apenas o conteúdo do direito à privacidade, mas também o seu vocabulário, passando a ser denominada como “privacidade informacional”, “Proteção de dados pessoais” e autodeterminação informativa[232].

Sobre o conceito de autodeterminação informativa, traz-se a colação de Ana Rosa Gonzáles Morua:

> "(…) se refiere al derecho de todas las personas a controlar el flujo de informaciones que a él le conciernen - tanto en la recolección como el posterior tratamiento y uso de los datos personales - mediante toda una serie de derechos subjetivos como el consentimiento, el derecho de acceso, rectificación"[233].

Em suma, o grande processamento de dados a partir da década de 70 do século XX resulta na evolução do conceito de privacidade, que passar a abranger o campo da proteção dos dados pessoais, destacando-se o controle da pessoa humana em relação ao fluxo de suas informações na sociedade.

No Brasil, o desenvolvimento da prática jurídica nas últimas décadas sugere uma evolução no conceito de privacidade, inclusive com a aplicação de diversos princípios relacionados à proteção de dados pessoais concretizados na doutrina internacional. No âmbito das iniciativas legais observa-se que a proteção da privacidade há muito é objeto de proteção pela Lei Ordinária: a lei dos *Habeas Data*, a Lei de arquivos Públicos, o Código Civil, o Código de Defesa do Consumidor, a Lei de acesso à informação, Lei de Cadastro Positivo, o Marco Civil da Internet, como o inciso X do artigo 5º da Constituição Federal.

---

232 MENDES. O direito..., *cit.*, p. 52.

233 GONZÁLES, Morua, Ana Rosa. ***Comentario a la S.T.C. 254/1993, de 20 de Julio. Algunas Reflexiones en torno al artículo 18.4 de la Constitución y la Protección de Datos Personales***, *in* Informática y Derecho nºs 6 y 7, Aranzadi, Mérida, 1994, pp. 243 - 244.

Nesse sentido, a evolução do conceito trata-se de um desenvolvimento natural do direito à privacidade, em decorrência das novas demandas originadas na sociedade de informação. O direito à autodeterminação informativa para a proteção dos dados pessoais encontra a sua base nos princípios gerais, que devem inspirar e incentivar o tratamento de dados pessoais. O seu cumprimento garante uma utilização racional e razoável dos dados pessoais, o que permite conciliar o desenvolvimento informático e as necessidades sociais com o pobre respeito escrupuloso dos direitos e liberdades do povo. Por isso, por meio da configuração dos princípios de proteção de dados, o legislador procura estabelecer um sistema preventivo de tutela da pessoa frente ao tratamento da informação que lhe diz respeito, estabelecendo um equilíbrio saudável e saudável entre a sociedade da informação.

3. HOMEM DE VIDRO: DEBATE ENTRE LIBERDADE E PRIVACIDADE

A sociedade da informação, conforme visto em momento anterior, é também uma sociedade da vigilância e da transparência. Os avanços das tecnologias de informação e comunicação e a estruturação político-econômica baseada em gerenciamento de informações traz riscos para a privacidade, cuja construção teórica e protetiva remete ao movimento iluminista. Com isto, há uma situação de possível regressão protetiva da vida privada em prol de uma alegada liberdade e utilidade.

Anteriormente, deve-se fazer uma breve explanação sobre liberdade e privacidade na modernidade.

A liberdade consiste na possibilidade de o indivíduo decidir livremente sobre o seu arbítrio e de agir conforme sua vontade própria, restringindo a ingerência de outras pessoas privadas ou públicas. O conceito é aqui adotado em sentido amplo, sem direcionar para uma modalidade específica de liberdade individual, a exemplo da liberdade contratual e de expressão. Ou seja, consiste na impossibilidade de limitação do arbítrio individual, exceto por lei e pela afetação da liberdade de outrem. Desta forma, está alinhada com a democracia, que traz as condições de possibilidade de seu exercício[234].

Conforme visto anteriormente, a privacidade diz respeito à proteção à vida privada. O direito à vida privada, como visto nos tópicos anteriores, limita a intervenção dentro de aspectos pessoais[235]. Este não se confunde com a tutela de dados pessoais, de extrema relevância no

[234] ROUANET, Luiz Paulo. **Sobre o caráter "abstrato" da democracia deliberativa**. Trans/Form/Ação, Marília, v. 36, n. spe, p. 177-194, 2013. Disponível em <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0101-31732013000400011&lng=pt&nrm=iso>. Acesso em 13 nov. 2020.
[235] RODOTÀ, Stefano. A **vida na sociedade de vigilância:** a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 8.

informacionalismo, a qual se refere à definição do tratamento de dados privados, determinando quanto ao grau de interferência externa e às condições para tanto[236]. Isto é, a proteção de dados pessoais está relacionada com a tutela da própria pessoa e de sua identificação.

Ambos os princípios mencionados estão na base axiológica do processo de modernidade, caracterizado pela racionalização da compreensão de mundo e pela secularização[237]. A ascensão da razão como forma de significação e de alicerce dos sistemas resultou em uma modificação da estrutura das instituições tradicionais, principalmente, no Estado nacional. Este se torna, na modernidade, um aliado do capitalismo e dos fenômenos resultantes deste, fundamentado e limitado por um ordenamento jurídico.

A modernidade teve como um dos seus efeitos a estruturação de quatro dimensões institucionais: o capitalismo; o industrialismo; o poder militar; a vigilância[238]. O capitalismo consiste no modelo econômico que influencia o aspecto político, produtivo e social, a partir da acumulação de capital[239]. O industrialismo, por sua vez, envolve a transformação de natureza de forma objetiva com o uso de tecnologias, e está imbricado com o capitalismo. As duas dimensões são essenciais para a modernidade e ditaram a própria formação do Estado nacional e a relação do homem com o seu ambiente. Há a ainda o poder militar, que se estrutura com base no monopólio dos mecanismos de violência pelo Estado, produtos da industrialização[240].

E, por fim, há a vigilância, a qual tem se intensificado com as novas tecnologias de informação e comunicação. Esta se sustenta em dois aspectos, o controle da informação e a supervisão social[241]. Neste sentido,

> A vigilância se refere à supervisão das atividades da população súdita na esfera política — embora sua importância como uma base do poder administrativo não se confine a esta esfera. A supervisão pode ser direta (como em muitas das instâncias discutidas por Foucault, tais como prisões, escolas e locais de trabalho abertos) mas, mais caracteristicamente, ela é indireta e baseada no controle da informação[242].

A vigilância se refere à relação do Estado com os cidadãos e o seu grau de ingerência no exercício do poder administrativo, monitorando a população e controlando os dados de

---

[236] RODOTÀ, Stefano. A **vida na sociedade de vigilância:** a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 8; MAGRANI, Eduardo. **Entre dados e robôs: ética e privacidade na era da hiperconectividade.** 2 ed. Porto Alegre: Arquipelágo, 2019, p. 36.

[237] A secularização consiste na separação entre a religião, expressa anteriormente como um valor ético-moral, e as demais esferas da vida. Desta forma, o Direito se centra numa perspectiva racional, centrada no ser humano, assim como a estrutura estatal.

[238] GIDDENS, Anthony. **As consequências da modernidade**. São Paulo: Editora Unesp, 1991, p. 70-71.

[239] GIDDENS, Anthony. **As consequências da modernidade**. São Paulo: Editora Unesp, 1991, p. 71.

[240] GIDDENS, Anthony. **As consequências da modernidade**. São Paulo: Editora Unesp, 1991, p. 71-72.

[241] GIDDENS, Anthony. **As consequências da modernidade**. São Paulo: Editora Unesp, 1991, p. 71.

[242] GIDDENS, Anthony. **As consequências da modernidade**. São Paulo: Editora Unesp, 1991, p. 69-70.

forma indireta. Tais ferramentas possibilitam a manipulação e a transparência dos cidadãos[243]. Contudo, não se limita à esfera estatal. Na modernidade, a vigilância é utilizada também por outras instituições, como empresas, redes sociais e organismos internacionais, estando vinculada com o capitalismo e o industrialismo. E, com isto, recorda-se aqui a abordagem de Manuel Castells[244] sobre informacionalismo que vislumbra a relação do desenvolvimento tecnológico da gestão de informação com a estruturação econômica a partir do processamento desta.

As organizações, independentemente do caráter público ou privado, se alicerçam, na modernidade, no gerenciamento e no controle de informações. O controle de informações é defendido dentro de uma suposta segurança, justificando uma redução da proteção ao direito à vida privada[245].

Vende-se a ideologia de que a sociedade da informação seria um novo iluminismo, trazendo mais informações e melhores decisões pelas pessoas e pelas entidades[246]. Entretanto, isto é necessariamente uma verdade, a hiperinformação implica em uma falta de verdade, de precisão[247]. Os efeitos da estrutura institucional baseada na vigilância e no processamento de informações vão além das *fake news* e do descrédito na ciência, tendo implicações em dois princípios pilares da modernidade, a liberdade e a privacidade.

Nesta direção, há uma tendência à exposição da esfera privada do indivíduo por vontade e liberdade própria, como um valor cultual a si mesmo, sem nenhum tipo de resistência à restrição à vida privada[248]. As redes sociais são os ciberespaços onde tal transparência mais ocorre como expressão da liberdade, sendo a pessoa um objeto-propaganda[249].

Desta forma, Han Byung-Chul[250] identifica a sociedade atual como sociedade da transparência, afetando os diversos aspectos do sistema social. Há a perspectiva de *post-privacy*[251], que não se limita apenas a limitação da privacidade, abrangendo uma mitigação da esfera privada[252].

---

[243] MOROZOV, Evgeny. **Big Tech**: a ascensão dos dados e a morte da política. São Paulo: Ubu Editora, 2018, p. 124.
[244] CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz e Terra, 1999, p. 54.
[245] RODOTÀ, Stefano. A **vida na sociedade de vigilância:** a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 8.
[246] MOROZOV, Evgeny. **Big Tech**: a ascensão dos dados e a morte da política. São Paulo: Ubu Editora, 2018; HAN, Byung-Chul. **Sociedade da transparência**. Petrópolis, RJ: Vozes, 2017, p. 18.
[247] HAN, Byung-Chul. **Sociedade da transparência**. Petrópolis, RJ: Vozes, 2017, p. 25.
[248] HAN, Byung-Chul. **Sociedade da transparência**. Petrópolis, RJ: Vozes, 2017.
[249] HAN, Byung-Chul. **Sociedade da transparência**. Petrópolis, RJ: Vozes, 2017, p. 31.
[250] HAN, Byung-Chul. **Sociedade da transparência**. Petrópolis, RJ: Vozes, 2017, p. 11.
[251] Dentro da ideologia em questão, compreende-se que a era digital trouxe o fim da privacidade, de forma que o indivíduo não tem mais como possuir segredos.
[252] HAN, Byung-Chul. **Sociedade da transparência**. Petrópolis, RJ: Vozes, 2017, p. 14.

Diante do cenário em questão, Evgeny Morozov[253] entende que a sociedade em questão traz uma emancipação predatória, cuja ideologia está na ampliação do uso e na facilitação do cotidiano. Todavia, esta utilidade tem um ponto negativo constantemente esquecido dentro da busca pela exposição e pelo exercício da liberdade, a redução da privacidade. Com efeito, não se pode afirmar que a sociedade da informação resulta em um novo esclarecimento pela razão[254].

A sociedade da informação é, em última instância, uma sociedade de vigilância, de controle e de transparência, em que o indivíduo, no exercício de sua liberdade, entrega sua esfera privada em prol do culto a si mesmo, da facilitação do dia a dia e da inserção social.

No momento de ingresso em uma plataforma online ou na aquisição de um serviço, a pessoa abdica parcialmente da salvaguarda em questão, em função de um uso, uma utilidade. No uso de um aparelho eletrônico, isto também ocorre. Para a participação em políticas públicas, se verifica o mesmo padrão. A participação e integração à sociedade de informação requer, deste modo, a relativização em determinado grau da privacidade, mais especificamente da proteção de dados pessoais quando se trata do meio digital.

Por conseguinte, o indivíduo não consegue mais manter informações e dados em segredo. A exposição e a transparência são base para a vigilância das instituições na modernidade, que se pautam em uma espécie de panóptico digital sem um centro soberano de controle. O Estado adentra, na sociedade em questão, a uma espécie de Big Brother distópico como no livro "1984" de George Orwell. Quem possui tal aptidão são as instituições que dominam o *know-how* das tecnologias de informação e de comunicação (TICs), como o Facebook, a Microsoft e a Apple.

Sobre este aspecto, Yuval Noah Harari discorre no seu livro "Homo Deus, Uma Breve História do Amanhã" sobre os riscos do avanço das TICs, os algoritmos, a privacidade e a vigilância. Neste sentido, em 2016, o autor concedeu uma entrevista em Madrid ao El País e destacou o seguinte:

> "Mas, no século XXI, estamos adquirindo mais conhecimentos biológicos e os computadores têm mais poder. Assim, o que a KGB era incapaz de controlar, o Facebook e a Apple conseguirão em… 10, 20 ou 30 anos? Poderiam monitorar seu corpo com sensores biométricos, registrar esses dados e, com algoritmos sofisticados, analisá-los para saber exatamente quem você é, sua personalidade, o que você gosta, que resposta daria a determinada pergunta. Quando uma entidade externa te entende melhor que você mesmo, não há mais livre-arbítrio"[255].

---

[253] MOROZOV, Evgeny. **Big Tech**: a ascensão dos dados e a morte da política. São Paulo: Ubu Editora, 2018, p. 170-171.

[254] HAN, Byung-Chul. **Sociedade da transparência**. Petrópolis, RJ: Vozes, 2017, p. 91.

[255] HARARI, Yuval Noah. Facebook e Apple poderão ter o controle que a KGB nunca teve sobre os cidadãos. [Entrevista concedida a] Cristina Galindo. **El País**, São Paulo, 13 nov. 2016. Disponível em:<https://brasil.elpais.com/brasil/2016/10/27/internacional/1477578212_336319.html>. Acesso em 18 de janeiro de 2021.

Frente ao panorama social, econômico e político elucidado acima, Stefano Rodotà[256] utiliza a expressão *homem de vidro,* uma metáfora usada para tratar do sistema nazista, em que diminuía à privacidade em prol de uma alegada segurança. Para o autor, a excessiva vigilância e transparência pelas instituições pode gerar o retorno do *homem de vidro,* em função do avanço dos sistemas de controle social[257].

No tocante ao Estado, a situação se torna mais gravosa, já que este tem o monopólio dos meios de violência. A utilização dos mecanismos de vigilância contra os cidadãos, baseada numa motivação de segurança nacional, implica a aproximação aos regimes totalitários, que interferem na vida privada da população. O controle de informação e a supervisão social viola a liberdade e a privacidade, se aproximando de um estado de exceção. Neste passo, há a necessidade do estabelecimento de regras para a proteção da dignidade da pessoa humana, tanto contra o Estado quanto contra as demais instituições.

Por outro lado, o indivíduo abdica da esfera privada, por si mesmo, em face da necessidade de exposição, como um imperativo moral e econômico[258]. Por conseguinte, não há violação à liberdade, já que o próprio homem o faz, sem nenhum tipo de coação[259].

Dentro da sociedade da informação, há a dicotomia entre privacidade e liberdade na relação entre o cidadão e o Estado e com outras instituições, assim como no próprio exercício da vontade do indivíduo. Há o exercício da liberdade pelo indivíduo limitando sua própria privacidade para se integrar nesta sociedade. Concomitantemente, também ocorre a restrição de ambos os axiomas pela vigilância estatal. Deste modo, não há propriamente um embate entre liberdade e privacidade, pois, na perspectiva individual, uma é a base para a relativização da outra e, no âmbito do controle do Estado, ambas são violadas.

Todavia, a tecnologia se demonstra como uma grande facilitadora da vida moderna, auxiliando no cotidiano, desde as tarefas mais simples às mais complexas. Desta forma, a abolição ou o regresso das TICs não aparece como uma solução para o panorama presente. É imprescindível impor limites e condições para o uso consciente e seguro destas. Neste passo, no próprio tópico, vislumbram-se possibilidades para a inserção no meio digital com a mitigação dos riscos à liberdade, à privacidade e à tutela de dados pessoais, a partir da abordagem da cidadania digital.

---

[256] RODOTÀ, Stefano. A **vida na sociedade de vigilância:** a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 8-9.
[257] RODOTÀ, Stefano. A **vida na sociedade de vigilância:** a privacidade hoje. Rio de Janeiro: Renovar, 2008, p.9.
[258] HAN, Byung-Chul. **Sociedade da transparência**. Petrópolis, RJ: Vozes, 2017, p. 113.
[259] HAN, Byung-Chul. **Sociedade da transparência**. Petrópolis, RJ: Vozes, 2017, p. 115-116.

4. CIDADANIA DIGITAL

Quando se trata da cidadania na modernidade, possui uma conotação relacionada com a esfera pública, já que perpassa pelo uso da opinião de forma pública[260], nos processos de tomada de decisão sobre assuntos de interesse público. Depende da criação de espaços de comunicação, livre de coações interna e externa, voltados para o entendimento, possibilitando a autodeterminação dos concernidos sobre temas de seu interesse[261].

A cidadania, neste passo, consiste na condição de cidadão de um Estado, que permite a sua participação nas tomadas de decisão. Deste modo, a cidadania materializa o direito de participação na esfera pública relativa aos temas políticos de um Estado. Contudo, o termo em tela não está restrito a tal abordagem, sendo visto como a possibilidade de viver como um cidadão e gozar da vida digna atribuída a este[262]. Ou seja, depende da institucionalização de mecanismos para a efetiva participação e deliberação popular.

Atem-se, no presente artigo, a uma conjunção de ambos os conceitos de cidadania anteriormente trazidos, de forma que a condição de cidadão possibilita a efetivação da dignidade da pessoa humana para o indivíduo inserido em uma comunidade jurídica, a qual concretiza a capacidade de participação na vida política da sociedade.

A cidadania digital é definida, por Karen Mossberger, Caroline J. Tolbert e Ramona S. Mc Neal [263], como a "aptidão de participação na sociedade online"[264]. Analisando o conceito de cidadania e a conceituação trazida, deve-se entender por cidadania digital a capacidade de participação no ambiente virtual, mediante a efetivação das condições de possibilidade para que seja consciente e segura.

Neste passo, infere a necessidade de integração e de acesso do meio digital, o que deve ser realizado a partir do acesso universal à internet e a eletrônicos de acesso à rede de computadores. Entretanto, não se limita a este aspecto, requer-se que a utilização do meio digital seja com consciência e segurança. Isto é, é imperioso que o usuário tenha a devida compreensão da forma de uso, das responsabilidades e dos riscos envolvidos

---

[260] Por esfera pública, se compreende aqui no texto como o local de legitimação do poder público com a opinião pública. Dentro deste ambiente, há a participação e a deliberação a partir da argumentação. HABERMAS, Jürgen. **Mudança estrutural da esfera pública: investigações quanto a uma categoria da sociedade burguesa**. Rio de janeiro: Tempo Brasileiro, 2003, p. 43.

[261] HABERMAS, Jürgen**. Direito e democracia**: entre facticidade e validade II . Rio de Janeiro: Tempo Brasileiro, 2011, p. 93.

[262] MARSHALL, T. H. **The Problem Stated with the Assistance of Alfred Marshall**. *In:* MARSHALL, T. H, BOTTOMORE, T. Citizenship and Social Class, pp. 3-51. Londres, Inglaterra: Pluto Perspectives, 1992, p. 8.

[263] MOSSBERGER, Karen. **Digital citizenship**: the internet, society, and participation. Londres, Inglaterra: Massachusetts Institute of Technology, 2008, p. 1.

[264] Tradução nossa.

Desta forma, a cidadania digital requer dois fatores: a inclusão digital e a educação digital, que serão mais bem delineados em seguida.

A inclusão digital consiste no processo de democratização e inserção nas tecnologias de informação e de comunicação, ampliando o acesso a estas e universalizando-o. A exclusão digital só pode ser combatida com auxílio de políticas públicas de integração da população ao meio digital, principalmente em uma sociedade desigual, como a brasileira. A atuação positiva do Estado é essencial para a promoção da justiça social e da inclusão, bem como para a ampliação do acesso à internet e aos meios eletrônicos. Para tanto, são listadas algumas medidas estatais: a redução de valores de equipamentos e de provedores de internet por meio da ampliação da concorrência no mercado; a educação e conscientização sobre o uso meio digital.

Sobre a educação digital, envolve a criação de currículos escolares com aulas de informática, a capacitação de professores e de servidores públicos para o uso do meio digital e a conscientização da população sobre a utilização segura da internet. Ademais, deve-se esclarecer os riscos para a segurança de dados pessoais, a liberdade e a privacidade envolvidos no uso das redes, promover o acesso às TICs de forma cautelosa e atenta,

No entanto, deve-se enfrentar as barreiras vistas no tópico anterior para a implementação da cidadania digital. Ou seja, é imprescindível a proteção à privacidade e o respeito ao direito à vida privada.

CONSIDERAÇÕES FINAIS

A sociedade da informação é caracterizada pelo processamento de informações como racionalidade, tanto do sistema econômico quanto do administrativo. Desta forma, sustenta-se nas tecnologias de informação e comunicação, bem como no capitalismo e no industrialismo. Com isto, trouxe uma série de facilidades e utilidades para a população em geral e permitiu um atendimento mais especializado para os consumidores.

Todavia, a facilitação mencionada possui um custo, a utilização de dados pessoais e a relativização da privacidade dos usuários. Surgiu, assim, a necessidade do fortalecimento da tutela de dados pessoais, em face da dicotomia presente entre liberdade e privacidade. O indivíduo, para se inserir na sociedade da informação, deve utilizar sua liberdade e abdicar parcialmente de sua privacidade e da tutela de seus dados, em razão da vigilância. Neste passo, fala-se em sociedade da transparência, sociedade da vigilância ou ainda em homem de vidro.

Diante deste cenário, é necessário a realização da cidadania digital, voltada para a inserção do indivíduo no meio digital, sua capacitação e sua educação. Em face da dificuldade

de regulamentação do tema, deve-se voltar-se para a conscientização do usuário sobre o uso das tecnologias de informação e comunicação e seus riscos.

REFERÊNCIAS

CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz e Terra, 1999.

GIDDENS, Anthony. **As consequências da modernidade**. São Paulo: Editora Unesp, 1991.

HABERMAS, Jürgen**. Direito e democracia**: entre facticidade e validade II . Rio de Janeiro: Tempo Brasileiro, 2011.

HABERMAS, Jürgen. **Mudança estrutural da esfera pública: investigações quanto a uma categoria da sociedade burguesa**. Rio de janeiro: Tempo Brasileiro, 2003.

HAN, Byung-Chul. **Sociedade da transparência**. Petrópolis, RJ: Vozes, 2017.

HARARI, Yuval Noah. Facebook e Apple poderão ter o controle que a KGB nunca teve sobre os cidadãos. [Entrevista concedida a] Cristina Galindo. **El País**, São Paulo, 13 nov. 2016. Disponível em:<https://brasil.elpais.com/brasil/2016/10/27/internacional/1477578212_336319.html>. Acesso em 18 de janeiro de 2021.

MAGRANI, Eduardo. **Entre dados e robôs: ética e privacidade na era da hiperconectividade.** 2 ed. Porto Alegre: Arquipelágo, 2019.

MARSHALL, T. H. **The Problem Stated with the Assistance of Alfred Marshall**. *In:* MARSHALL, T. H, BOTTOMORE, T. Citizenship and Social Class, pp. 3-51. Londres, Inglaterra: Pluto Perspectives, 1992.

MOROZOV, Evgeny. **Big Tech**: a ascensão dos dados e a morte da política. São Paulo: Ubu Editora, 2018.

MOSSBERGER, Karen. **Digital citizenship**: the internet, society, and participation. Londres, Inglaterra: Massachusetts Institute of Technology, 2008.

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

ROUANET, Luiz Paulo. **Sobre o caráter "abstrato" da democracia deliberativa**. Trans/Form/Ação, Marília , v. 36, n. spe, p. 177-194, 2013 . Disponível em <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0101-31732013000400011&lng=pt&nrm=iso>. Acesso em 13 nov. 2020.

ESTUDO PRÉVIO DE ANÁLISE DE IMPACTO TECNOLÓGICO OPERADO POR INTELIGÊNCIA ARTIFICIAL: UMA PROPOSTA DE PROTEÇÃO À PRIVACIDADE EM UMA SOCIEDADE MONITORADA

Simone Souza[265]

Introdução

O avanço tecnológico que marca a sociedade moderna vem revolucionando a forma como as pessoas se comunicam, se socializam e adquirem conhecimento. As informações estão a um clique de distância, ainda que as pessoas em geral estejam pouco informadas ou indiferentes[266].

Nosso dia a dia anda abarrotado dessas tecnologias: smartphones, smartwatch, smart TV, e-mails, WhatsApp, Facebook, Instagram, LinkedIn, Twitter, PIX, biometria, se traduzem em produtos e serviços que têm mudado e exposto significativamente nossas vidas. Se por um lado trouxeram inúmeros benefícios, por outro, têm gerado um acúmulo exponencial de dados que podem apontar para uma realidade cada vez maior de vigilância e controle, capaz de transformar o homem em um "ser de vidro".

O ano de 2020 certamente ganhará um capítulo nos livros de história. A virtualização das relações e interações sociais, fenômeno que já era uma realidade onipresente no mundo pré-pandêmico, mas que se intensificou com as medidas de isolamento e distanciamento social impostas pela pandemia, trouxeram como um de seus efeitos a produção de um sem-número de novos dados, e, por uma estranha coincidência, no mesmo ano, a Lei geral de proteção de dados (LGPD) entra em vigor, embora de forma parcial e sem que a Autoridade estivesse estabelecida. Fato é que todos precisamos (e já deveríamos) nos adequar a ela.

A proteção à privacidade se traduz em interesse mundial, não faltando discussões acerca do tema e de seus correlatos. Entretanto, será que realmente podemos falar de privacidade em um mundo onde o consumo de nossos dados é realizado diuturnamente, frequentemente ao arrepio da nossa vontade? Para além do direito de estar só, é possível afirmar a existência ao

---

[265] Doutoranda em Direito, Instituições e Negócios pela Universidade Federal Fluminense – PPGDIN/UFF, Mestre em Sociologia e Direito pela Universidade Federal Fluminense – PPGSD/UFF, Especialista em Processo Civil pela Universidade Estácio de Sá. Pesquisadora do Laboratório Fluminense de Estudos Processuais – LAFEP, Membro da Associação Brasileira de Direito Processual - ABDPRO. Membro da Associação Nacional de Advogados de Direito Digital - ANADD. Associada do Instituto Nacional de Pesquisa e Promoção de Direitos Humanos - INPPDH. Professora de Processo Civil.

[266] Dobour, Ladislaw. "Sociedade Vigiada: como a invasão da privacidade por grandes corporações e estados autoritários ameaça instaurar uma nova distopia". Editora: Autonomia Literária. 1ª ed. 2020, p. 3.

direito de preservação de nossas informações e de nossa própria dignidade diante de constante monitoramento? Temos realmente liberdade de escolha?

Com o aumento exponencial dos recursos tecnológicos, notadamente com a utilização de inteligência artificial[267] (IA), o mercado mudou e os dados tornaram-se a principal matéria prima para a confecção de produtos. Como diria Rodotà[268]: "Aumentou a pressão pela utilização de toda a espécie de dado pessoal, sobretudo por motivos de segurança interna e internacional, mas também para finalidades comerciais" A cada dia somos atropelados por inovações tecnológicas[269] sem que nem mesmo saibamos do que se trata ou de quem as detém. Homens de vidro desnudados ao mundo!!!!

Ao que parece, as medidas de isolamento e distanciamento social impostas pela pandemia mundial fez com que a dependência das ferramentas tecnológicas nos colocasse diante de uma questão maior: a total disponibilidade para manutenção das relações interpessoais e laborais. O mundo em sua quase totalidade tornou-se virtual e com isso, mais de nossos dados passaram a constar na rede! Nas lições de Rodotà, em tempos de crise, acabamos por relativizar nossos direitos individuais[270]. Fato que é dispomos de nossa individualidade em prol de nos mantermos seguros isoladamente.

Conveniente ou não, esse momento acabou ratificando a facilidade com que a comunicação pode ocorrer, a proximidade que a rede pode trazer e, por fim, reverberou em avanços gigantescos como, por exemplo, o *e-comerce*[271] e startups. Conforme noticiado por

---

[267] De forma resumida, inteligência artificial é um campo de estudo da ciência da computação cujo objetivo é criar algoritmos que imitem o funcionamento do cérebro humano. A inteligência artificial (IA) possibilita que máquinas aprendam com experiências, se ajustem a novas entradas de dados e performem tarefas como seres humanos. A maioria dos exemplos de IA sobre os quais você ouve falar hoje – de computadores mestres em xadrez a carros autônomos – dependem de deep learning e processamento de linguagem natural. Com essas tecnologias, os computadores podem ser treinados para cumprir tarefas específicas ao processar grandes quantidades de dados e reconhecer padrões nesses dados. Para aprofundamento no tema vide RUSSELL, Stuart Jonathan; NORVIG, Peter. "Inteligência artificial". tradução Regina Célia Simille. – Rio
de Janeiro: Elsevier, 2013; LEE, Kai-Fu. "Inteligência artificial: como os robôs estão mudando o mundo, a forma como amamos, nos comunicamos e vivemos". Tradução Marcelo Barbão. 1ª ed. Rio d Janeiro: Globo livros, 2019. SAS Insights disponível em <https://www.sas.com/pt_br/insights/analytics/what-is-artificial-intelligence.html> Acesso 14/11/2020.

[268] Idem.

[269] Stefano Rodotà já expressava essa preocupação ao afirmar que a união entre áreas do saber, atreladas às incessantes inovações científicas e tecnológicas, parecem tornar vã qualquer pretensão de oferecimento de uma tutela jurídica. (RODOTÁ, Stefano. "A vida na sociedade da vigilância – a privacidade hoje". Org. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Ed. Renovar, 2008, p. 243).

[270] Idem, p. 56.

[271] MOTA, Renato. "Retrospectiva 2020: ano do e-commerce e avanço dos meios de pagamento". *In* Olhar Digital, 22/12/2020. Disponível em <https://olhardigital.com.br/2020/12/22/retrospectiva-2020/retrospectiva-2020-ano-do-e-commerce-e-avanco-dos-meios-de-pagamento/?gfetch=2020%2F12%2F22%2Fretrospectiva-2020%2Fretrospectiva-2020-ano-do-e-commerce-e-avanco-dos-meios-de-pagamento%2F> Acesso 03/01/2021.

Gilberto Sarfati, professor da FGV-SP, em reportagem feita por Capelas e Wolf[272]: “É muito positivo o balanço de 2020 até aqui. É quase como se o ecossistema estivesse à margem da crise que se vive no Brasil [...]"A digitalização já ganharia destaque de qualquer jeito a médio prazo, mas a crise acelerou o processo."

Se por um lado a pandemia acelerou inovações tecnológicas e ampliou a utilização da rede, por outro, trouxe uma questão ainda maior traduzida não apenas na coleta massiva de dados, mas, sobretudo, no debate concernente à privacidade em uma sociedade de vigilância.

Uma das principais características de Stefano Rodotà, a lhe conferir singularidade e originalidade, era o interesse que tinha no sujeito concreto, real, e não no sujeito abstrato da dogmática. Nesse sentido a presente pesquisa se volta para analisar o impacto que o avanço tecnológico, notadamente com uso de inteligência artificial, pode trazer à questão da privacidade na sociedade contemporânea.

Muito embora em algum momento possa o presente artigo não parecer jurídico, tais questões expostas implicam a necessidade de refletirmos acerca de limites éticos e de regulações, que venham a delinear até que ponto as tecnologias operadas por inteligência artificial devam ir. Esta era uma preocupação ponderada por Rodotà ao retornar às salas de aula com a disciplina de Tecnologias e direitos.

Como apresenta Maria Celina Bodin de Moraes, ainda que perecessem ser questões marginais, que com direito pouco teria relação, torna-se perceptível que temas ligados a bioética e a informática passaram não apenas a temas capitais para pesquisa dos juristas, mas que transformaram profundamente também o modo como jurista olha a realidade[273].

O presente artigo não tem a pretensão de esgotar o tema, mas de mostrar como a privacidade tem sido trabalhada nos Estados Unidos, Europa e Brasil e o quanto suas diretivas podem ou não serem compatíveis com algumas tecnologias de monitoramento que estão sendo desenvolvidas e inseridas no mercado.

A metodologia adotada nesse artigo conta com pesquisa bibliográfica a partir da análise da obra de Stefano Rodotà, com ênfase no monitoramento a configurar uma sociedade da vigilância, com ampla coleta de dados pessoais, conectando o emprego de tecnologias à necessidade de proteção à privacidade como um direito fundamental à dignidade.

---

[272] CAPELAS, Bruno; WOLF, Giovanna. “Mercado de startups do Brasil caminha para ter melhor ano da história em 2020”. *In* Estadão. Out/2020. Disponível <https://economia.uol.com.br/noticias/estadao-conteudo/2020/10/26/mercado-de-startups-do-brasil-caminha-para-ter-melhor-ano-da-historia-em-2020.htm?cmpid=copiaecola> Acesso 14/12/2020.

[273] Stéfano Rodotà, Op. cit. Apresentação do autor e da obra, p. 4.

A Privacidade na Sociedade da Informação

Do conceito da privacidade na dimensão privada e pública

A dimensão da privacidade não se restringe mais "ao direito de estar só", expressão utilizada pela primeira vez em 1880 pelo Thomas Cooley[274], e que ganhou novos contornos aos ser relacionada à noção de privacidade no ano de 1890, com a publicação do artigo de Warren e Brandeis, na Harvard Law Review, intitulado "*The Right to Privacy*", ao lecionarem[275]:

> Invenções recentes e métodos de negócios chamam a atenção para o próximo passo que deve ser dado para a proteção da pessoa e para assegurar ao indivíduo o que o juiz Cooley chama de direito de "ser deixado em paz". Fotografias instantâneas e empreendimentos de jornais invadiram os recintos sagrados da vida privada e doméstica; e numerosos dispositivos mecânicos ameaçam cumprir a previsão de que "o que se sussurra no armário será proclamado do alto das casas". Durante anos, houve um sentimento de que a lei deve fornecer algum remédio para a circulação não autorizada de retratos de pessoas privadas; e o mal da invasão de privacidade pelos jornais, sentido há muito tempo, foi discutido recentemente por um escritor competente. Os fatos alegados de um caso um tanto notório levado a um tribunal inferior em Nova York há alguns meses, envolveram diretamente a consideração do direito de retratos em circulação; e a questão de saber se nossa lei reconhecerá e protegerá o direito à privacidade neste e em outros aspectos deve ser levada em breve aos nossos tribunais para consideração. (Tradução livre)

Após mais de um século, a preocupação de Warren e Brandeis ressoa contemporânea. Na realidade, ainda que a dimensão do conceito de privacidade nos últimos anos não se volte unicamente para a esfera individual, mas, precipuamente para a esfera pública, a preocupação

---

[274] Antes do artigo de Warren e Brandeis, é possível encontrar na obra do juiz Thomas Cooley, publicada em 1880, sob o título "*A treatise on the laws of Torts*" a primeira utilização da expressão "*right to bel et alone*". E, muito embora tenha cunhado a expressão, Cooley não a relacionou com a noção de privacidade, mencionando-a em seu trabalho de responsabilidade civil como parte do seguinte trecho: "*the right to one's person may be said to be a right of complete immunity: to bem alone*". (ZANINI, Leonardo Estevam de Assis. "O surgimento e o desenvolvimento do *right to privacy* nos Estados Unidos". *In* Revista Jus Navigandi, Teresina, ano 22, n. 5130, 18/07/2017. Disponível em <https://jus.com.br/artigos/57228> Acesso 04/01/2020.

[275] "*Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone" [10] Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops." For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons;[11] and the evil of invasion of privacy by the newspapers, long keenly felt, has been but recently discussed by an able writer.[12] The alleged facts of a somewhat notorious case brought before an inferior tribunal in New York a few months ago,[13] directly involved the consideration of the right of circulating portraits; and the question whether our law will recognize and protect the right to privacy in this and in other respects must soon come before our courts for consideration*". WARREN, Samuel D.; BRANDEIS, Louis D. "The Right to Privacy". *In* Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220, p. 195. Disponível em <https://www.jstor.org/stable/1321160?seq=1#metadata_info_tab_contents> Acesso 08/08/2020.

de Warren e Brandeis poderia figurar (e figuram), com pequenas adaptações, nas doutrinas jurídicas da atualidade. As inquietações de hoje são as mesmas. Contudo, as inovações tecnológicas são um tanto distintas, são detentoras de poderes de intrusão deveras maior e, na maioria das vezes imperceptíveis quanto ao resultado que podem alcançar.

Nessa seara de inovações e violações, Stefano Rodotà, em obra publicada apenas no Brasil, traçou um panorama acerca do que existia e do quanto deveríamos nos debruçar, não para romper ou evitar os avanços tecnológicos (seria simplesmente impossível), mas, para fazer com que, a esses avanços, fossem conferidos limites de utilização pelo homem e não pela máquina. A mera disponibilidade de uma tecnologia não pode legitimar toda sua funcionalidade[276].

No cenário atual há uma verdadeira governança por grandes organizações tecnológicas como Amazon, Facebook, Instagram, WhatsApp, Google etc. Somos influenciados pelo uso diário e contínuo que fazemos dos serviços colocados à disposição e, que, falaciosamente são oferecidos a título gratuito, uma vez que a moeda de troca se traduz na coleta de nossos dados. Nesse sentido, Rodotà[277] afirma que:

> Concretamente, isso significa que a contrapartida necessária para se obter um bem ou um serviço não se limita mais à soma de dinheiro solicitada, mas é necessariamente acompanhada por uma cessão de informações. Nessa troca, então, não é somente o patrimônio de uma pessoa que está envolvido. A pessoa é obrigada a expor seu próprio eu, sua própria *persona*, com consequências que vão além da simples operação econômica e criam uma espécie de posse permanente da pessoa por parte de quem detém as informações a seu respeito.

Desta forma, há, portanto, de um lado uma governança sobre nossas vidas, e de outro, verdadeiro monopólio de dados a gerar, por consequência, o esvaziamento de direitos, uma vez que ao ser tolhida nossa privacidade, também nossa liberdade de expressão e nossa participação serão tolhidas. Assim a caracterização da nossa organização social, como uma sociedade cada vez mais baseada na acumulação e circulação de nossas informações, aponta Rodotà, comporta a origem de um novo e verdadeiro recurso de base, ao qual atrela novas situações de poder[278].

Nas sociedades de informação, como se mostra a sociedade em que vivemos, “nós somos as nossas informações", uma vez que por elas somos definidos, classificados, etiquetados e, portanto, ter como controlar a circulação das informações e saber quem as usa significa adquirir, concretamente, um poder sobre si mesmo[279].

---

[276] Rodotà, Stefano. Op. cit. p. 241.
[277] Idem, p. 113.
[278] Idem, p. 36.
[279] Idem, pp. 114-115.

A importância da privacidade atualmente não mais restringe-se ao direito de ser deixado em paz, como defendido por Warren e Brandeis, mas, se volta em relação ao espaço que ocupamos, às nossas informações dentro desse espaço público do qual fazemos parte. Se é possível obter uma defesa da privacidade individual, não se coloca em discussão a lógica da vigilância, que passa a ser transferida do indivíduo ao grupo. As tecnologias da comunicação e da informação manifestam-se assim no sentido de se construir livremente a própria esfera privada, entendida como autodeterminação informativa, como poder de controlar a circulação das próprias informações[280].

Nas lições de Rodotà[281], mudam-se os sujeitos que solicitam a defesa da privacidade e a própria qualidade de seu pleito. Privilegiando a defesa frente as modalidades de exercício do poder por parte de detentores públicos e privados de suas informações, a invocação da privacidade supera a dimensão individual e dilata-se em uma dimensão coletiva, já que não se leva em consideração o interesse do indivíduo enquanto tal, mas, como pertencente a um determinado grupo social.

A privacidade é um direito humano inerente e um requisito para manter a condição humana com dignidade e respeito. É uma questão de escolha e de ter o poder de controlar como você se apresenta ao mundo[282]. Configura-se, portanto, como um direito fundamental à própria dignidade. Há que se considerar esse conceito de individualidade, de particularidade, de singularidade, de intimidade que não pode ser invadida seja a que pretexto for. O direito à privacidade é uma condição para a realização do ser humano como ser livre e autônomo, em toda a sua plenitude[283].

Nas lições de Rodotà[284], devemos entender como privacidade o "direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada", de forma a ser vista como o direito a autodeterminação informativa.

Sociedade da Informação e a importância dos dados: a Teoria do Mosaico

Para quem importaria meus dados? Esta é uma pergunta que podemos nos fazer diariamente, e o principal motivo de muitos não se preocuparem. Entretanto, nada é efêmero na

---

[280] Rodotà, op. cit. 113.
[281] Idem, p. 30.
[282] SCHNEIER, Bruce. "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World". 1ª ed. W. W. Norton & Company, 2015, Ebook Kindle Amazon, cap. 10, n.p.
[283] MAFRA, Waldir Ap. "A privacidade como direito fundamental da pessoa humana". *In* Sociedade Vigiada: como a invasão da privacidade por grandes corporações e estados autoritários ameaça instaurar uma nova distopia. Editora: Autonomia Literária. 1ª ed. 2020, pp. 11-34, p. 15.
[284] Op. cit. p. 109.

vigilância por máquinas[285], o que não importa hoje pode ser de extrema relevância amanhã. Os dados coletados podem ser consultados sempre que o gestor do sistema considerar oportuno, com finalidades estatísticas, para planejar campanhas publicitárias, para traçar perfis dos usuários, como também podem ser cedidos a terceiros[286].

Com o advento da internet e a ampla utilização da rede, vários dados começaram a circular, aptos a viabilizar o armazenamento que, somado ao avanço tecnológico, notadamente com a inteligência artificial, torna possível alcançar resultados que humanamente seria impossível. A dimensão sócio-política de nossas vidas está sendo profundamente transformadas, e a relação de poder exercida em torno de nós culturais e conteúdo de informação, tendem a moldar o comportamento humano[287].

Assim, o sistema de informação atrelado à compreensão dessa nova matéria prima que são os dados, configura-se como um conjunto de componentes inter-relacionados que coleta, manipula, armazena e dissemina dados e informações e fornece mecanismo de realimentação (feedback) para atingir um objetivo[288]". Se os dados são o novo petróleo nessa sociedade da informação, o que seriam esses dados e quando seria obtida a informação? Seriam sinônimos? No que concerne a proteção à privacidade, de quais dados estaríamos a tratar?

Conforme nos ensina Stair e Reynolds[289]:

> Os dados consistem em fatos brutos, como o número de funcionários, horas totais trabalhadas em uma semana, números de peças no estoque ou pedidos de vendas. [...] Quando os fatos são organizados de maneira significativa, tornam-se informação. Informação é uma coleção de fatos organizados e processados de modo que tenham valor adicional, que se estende além do valor dos fatos individuais. [...] Transformar os dados em informação é um processo, ou um conjunto de tarefas logicamente relacionadas realizadas para alcançar um resultado definido. O processo de definir relações entre os dados para criar informações úteis requer conhecimentos. Conhecimento é a consciência e compreensão de um conjunto de informações e maneiras como essas informações podem ser úteis para apoiar uma tarefa específica ou para chegar a uma decisão.

---

[285] SCHNEIER, idem.
[286] RODOTÀ, op. cit. p. 112.
[287] CASTELLS, Manuel. "A galáxia da internet: reflexões sobre a internet os negócios e a sociedade". Tradução dos pontos Maria Luiza X. de A. Borges. Revisão técnica: Paulo Vaz. Rio de Janeiro: Jorge Zahar Ed., 2003, p. 135.
[288] STAIR, Ralph M.; REYNOLDS, George W. "Princípios de sistemas de informação". 3ª ed. Tradução da 11ª ed. Norte-Americana. Tradução: Noveritis do Brasil. Revisão Técnica: Tânia Fátima Calvi Tait. Editora: Cengage Learning; 2015, p. 4.
[289] Idem, p. 5-6.

De acordo com as lições de Doneda[290] o dado estaria associado a uma espécie de "pré-informação", anterior a interpretação e a um processo de elaboração; enquanto a informação, estaria a se referir a algo além da representação contida no dado, chegando ao limiar da cognição. Na informação é possível pressupor a correção de seu conteúdo, o que implica dizer que a informação carrega em si também um sentido instrumental, no sentido da redução de um estado de incerteza.

Desse modo uma informação depende do motivo pelo qual e para o qual será utilizada, o que nos remete ao fato de que dependerá de um interesse subjetivo daquele que lhe confere significado a partir do tratamento conferido aos dados. O que resta claro ao analisarmos documentários como “O dilema das redes” ou “Privacidade Hackeada” que demonstram, nitidamente, para quem aquelas informações interessavam e para qual finalidade.

Apesar de haver modalidades de dados e informações[291], a nós interessa, àqueles concernentes às pessoas (dados pessoais e dados sensíveis) e seus patrimônios, isso porque são essas informações que podem implicar violações à privacidade. Diante de uma sociedade da informação, como a que vivemos, não apenas é possível, como já é feita a coleta de grande parte de dados pessoais, seu processamento, agrupamento e sua relação das mais diversas formas realizando assim o tratamento desses dados.

Destarte, todo e qualquer dado pode ser importante no contexto da sociedade da informação. Elaborada por Fulgencio Madrid Conesa[292], a teoria do mosaico afirma que muito embora haja prioridades relevantes do ponto de vista do direito à privacidade, uma vez conectados outros dados, talvez irrelevantes, estes também possam servir para tornar totalmente transparente a personalidade de um cidadão, tal qual ocorre com pequenas pedras que formam os mosaicos. Ainda que aparentemente nenhuma importância possa ter, unidas formam um conjunto cheio de significados.

Note que o tratamento dos dados ou informações pessoais, isoladamente considerados podem não possuir caracter íntimo, mas, ao serem cruzados com outros dados ou informações, podem permitir a elaboração de perfis pessoais do indivíduo tal qual aponta a teoria do mosaico O autor assevera que ao reunir pequenos dados sem nenhum significado e ao estruturar de forma organizada será possível obter informações privilegiadas e mesmo íntimas daquela pessoa[293].

---

[290] DONEDA, Danilo César Maganhoto. “Da privacidade a proteção de dados pessoais: elementos da formação da lei geral de proteção de dados”. 2ª Ed. São Paulo: Thomson Reuters Brasil, 2020, p. 136.
[291] DONEDA, op. cit. p. 139.
[292] CONESA, Fulgencio Madrid. “Derecho a la intimidad, informática y Estado de Derecho”. Universidad de Valencia, Valencia, 1984, p.45.
[293] Ibidem.

E a pesquisa realizada por *Neguine Rezaii* comprova tal assertiva ao descobrir que a análise da linguagem pode prever com mais de 90% de precisão quais pacientes tem probabilidade de desenvolver esquizofrenia antes que quaisquer sintomas típicos possam surgir[294]

Com advento de tecnologias operadas por inteligências artificiais, se alcança, não apenas o armazenamento de um exponencial número de dados, mas, enorme capacidade de processamento para tratamento esses dados no sentido de organizar, cruzar, classificar e analisar, o que os tornam significativamente importantes tanto para a esfera governamental, quanto mais para a esfera privada, notadamente na obtenção de perfis que lhes permitam maiores estratégias de mercado.

Nas lições de Rodotà[295] ainda que normas proíbam a criação de perfis, estas são facilmente burladas pela ausência de auditorias prévias, nesse sentido:

> [...]os perfis são utilizados para decisões que, para a maioria dos cidadãos, são mais frequentes e, no mais das vezes, mais significativas do que as judiciais ou administrativas, e que são aquelas que dizem respeito ao cidadão consumidor ou usuário de serviços [...] tal preocupação aliás encontra-se na lei francesa que amplia a proibição também às decisões privadas. A eficácia de uma disposição como essa, todavia, é fortemente reduzida pelo fato de que pode ser fácil superar a proibição sustentando que a decisão não foi tomada somente a partir do perfil automatizado; e, sobretudo, que não se trata de decisões individuais, mas relativas a grupos ou categorias, e que a mera classificação de um indivíduo dentro de um desses grupos ou categorias não pode ser considerada tecnicamente uma decisão.

A grande questão apontada por Rodotà[296] é que a coleta e a circulação das informações ocorrem hoje em um contexto amplamente despersonalizado, no qual o respeito é sobrepujado por outras lógicas, e pela necessidade de a sociedade da informação[297] obter seu alimento. Para

---

[294] ADAM, David. "Machines can spot mental health issues—if you hand over your personal data". *In* MIT Technology Review, 13/08/2020, n.p. Disponível em <https://www.technologyreview.com/2020/08/13/1006573/digital-psychiatry-phenotyping-schizophrenia-bipolar-privacy/> Acesso em 20/09/2020.

[295] Op. cit. pp. 115-116.

[296] RODOTÀ, op. cit. p. 139.

[297] Para Pierre Levy, a sociedade de informação – ou sociedade do conhecimento – seria fruto de do conjunto de todos os impactos sócio-técnico-culturais da investigação, da inovação e do desenvolvimento científico e tecnológico digital. Todos estes fatores teriam propiciado as novas configurações sociais, que são próprias da atual cultura digital (LEVY, Pierre. "*Cibercultura".* Rubí (Barcelona) Editorial: México: Universidad Autónoma Metropolitana - Iztapalapa, 2007, p. 18. Apud RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. "O direito à proteção de dados pessoais na sociedade da informação". *In* Revista Direito, Estado e Sociedade. Programa de Pós-Graduação em Direito da PUC-Rio. n. 36, Jan/Jun2010, pp. 178-199, p. 179). Disponível em <https://revistades.jur.puc-rio.br/index.php/revistades/issue/view/22> Acesso 06/11/2020.

ele, uma verdadeira privacidade pode ser fundada somente em um profundo e sensível respeito recíproco dentro de uma dimensão ética.

À guisa de ilustração, muito embora vigente a Lei Geral de Proteção de Dados, desde agosto de 2020, recentemente o Tribunal de Justiça de São Paulo[298], determinou a suspensão da venda de informações pessoais de clientes pelo Serasa Experian que, segundo demanda promovida pelo Ministério Público do Distrito Federal, estaria ela realizando "comercialização maciça de dados pessoais de brasileiros por meio dos serviços 'Lista Online' e 'Prospecção de Clientes' que vendem dados como nome, CPF, endereço, idade, gênero, poder aquisitivo e classe social de pessoas que figuram em seu banco de dados, sem consentimento[299] específico dessas pessoas.

A linha mestra para o tratamento de dados pessoais é o consentimento livre e informado do titular, ainda que em alguns casos seja ele dispensado[300], e em não seja o consentimento a única exigência, como nos casos de dados sensíveis, mas o tratamento de dados informados deverá estar vinculado às finalidades apresentadas.

Breves considerações acerca da tutela à privacidade

Estados Unidos x União Europeia

Nos últimos anos tema central a marcar os debates foi a proteção de dados como garantia de privacidade, notadamente em virtude dos avanços tecnológicos e, recentemente, não só com a ampliação da utilização de sistemas operados por inteligência artificial, mas, sobretudo pelas medidas de isolamento e distanciamento social impostas pela pandemia que trouxe a lume a questão da liberdade x segurança.

A importância conferida à proteção de dados (tanto na dimensão da vida privada quanto na dimensão da liberdade), é mundial, excetuado os países Asiáticos, notadamente China, onde a vigilância social é frequente[301]; e é refletida pelos inúmeros documentos nacionais e

---

[298] Para maiores informações veja TJ-DF. Agravo De Instrumento. Processo nº.: 0749765-29.2020.8.07.0000 Agravante: Ministério Público do Distrito Federal e dos Territórios, Agravado: Serasa S.A. Relator: Desembargador Cesar Laboissiere Loyola. Decisão proferida em 20/11/2020.

[299] Dicção do art. 5º, XII, da Lei 13.709/18 – LGPD: Consentimento é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

[300] Art. 7º, § 4º, LGPD.

[301] A vigilância social é frequente graças a troca de dados entre os fornecedores da internet e de telefonia celular. Cerca de duzentas milhões de câmeras dotadas de inteligência artificial, captam imagens, observam e avaliam qualquer pessoa nos espaços públicos, lojas, ruas, estações e aeroportos. (HAN, Byung-Chul. "O coronavírus de hoje e o mundo de amanhã". *In* El País, 20/03/2020, n.p. Disponível em <https://brasil.elpais.com/ideas/2020-03-22/o-coronavirus-de-hoje-e-o-mundo-de-amanha-segundo-o-filosofo-byung-chul-han.html> Acesso em 03/01/2021.

internacionais, como a Carta de Direitos Fundamentais da Comunidade Europeia, na qual a proteção de dados é reconhecida como um direito fundamental autônomo[302].

O cenário atual, sobretudo pelo impacto do avanço tecnológico, colocou em pauta uma das distinções precípuas existentes entre o direito norte-americano e o direito Europeu na forma de proteção à privacidade. Isto porque, o acesso e tratamento exponencial de nossas informações através de inúmeras técnicas de monitoramento, nos aproxima da sociedade disciplinar retratada por Michael Foucault[303].

Muito embora sejam Warren e Brandeis considerados pais fundadores da privacidade no terreno jurídico [304], a evolução do sistema jurídico da *privacy* teve um enfoque predominantemente consumerista e principiológico, enquanto, na Europa, a base da privacidade partiu da dignidade, sendo tratada como direito fundamental. Inclusive a visão de privacidade como direito a autodeterminação informativa restou introduzida pela corte constitucional alemã em 1983[305].

Ainda que em ambos os ordenamentos as legislações tragam um certo grau principiológico, o consentimento, base do direito à autodeterminação informativa, na qual o indivíduo se mostra capacitado e informado o suficiente para exercer sua liberdade de decisão acerca do tratamento efetuado junto aos seus dados[306], é a estrutura precípua que diferencia o sistema de proteção. E ainda que o tratamento dos dados pessoais pressuponha o consentimento livre do titular, é na forma de desenvolvimento desse consentimento que se pauta as atuais reclamações americanas[307].

A doutrina do *Third party doctrine*[308], adotada nos Estados Unidos, sustenta que o mero fornecimento voluntário de suas informações a terceiros lhe retira a expectativa razoável de

---

[302] RODOTÀ, op. cit. p. 13.
[303] FOUCAULT, Michel. Vigiar e Punir: nascimento da prisão; tradução de Raquel Ramalhete. Petrópolis: Vozes, 1987, p. 162-187.
[304] RODOTÀ, op. cit. p. 28.
[305] Idem, p. 144.
[306] NOGUEIRA, Fernanda Araújo Couto e Melo; FONSECA, Maurício Leopoldino da. "O consentimento na Lei Geral de Proteção de Dados: autonomia privada e o consentimento livre, informado, específico e expresso". *In* Lei Geral de Proteção de Dados: Uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial [recurso eletrônico] Org. Bernardo Menicucci Grossi. Porto Alegre/ RS: Editora Fi, 2020, pp. 15-35. P. 22.
[307] SANTANA, Wesley. "Nos EUA, 87% consideram a privacidade de dados como um direito humano". *In* Olhar Digital, 07/08/2020, n.p. Disponível em <https://olhardigital.com.br/2020/08/07/noticias/nos-eua-87-consideram-a-privacidade-de-dados-como-um-direito-humano/> Acesso 04/12/2020.
[308] Para aprofundamento no tema veja KERR, Orin S. "The Case for the Third-Party Doctrine". *In* Michigan Law Review. Volume 107. Issue 4, 2009. Disponível em <https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1348&context=mlr>; STERN, Simon. "The Third-Party Doctrine and the Third Person". *In* New Criminal Law Review, vol. 16, 2013. pp. 101-147. Disponível em < https://tspace.library.utoronto.ca/bitstream/1807/87908/1/Stern%20Third%20Party%20Doctrine.pdf>; THOMPSON II, Richard M. The Fourth Amendment Third-Party Doctrine. *In* Congressional Research Service. 2014. Disponível em < https://fas.org/sgp/crs/misc/R43586.pdf> Acesso 30/11/2020.

privacidade, permitindo que os dados fornecidos possam ser amplamente utilizados. Apesar das inúmeras críticas, inclusive internas, sobre a necessidade de novos Princípios de proteção à privacidade do consumidor, o sistema consumerista e de regulação via FTC ainda se mantém como dominante nos EUA.

Como explica Bioni e Zanatta[309], no lugar de um modelo de leis gerais e Autoridades Nacionais de Proteção de Dados Pessoais como ocorre na União Europeia, os FIPPs - *Fair Information Practices Principles* foram internalizados na cultura decisória da *Federal Trade Commission*, que acabou por criar, ao longo de décadas de atuação, uma espécie de "common law" da privacidade.

A União Europeia, por sua vez, optou por definir limites, cujo início se deu com a diretiva 95/46, revogada pelo atual Regulamento Geral sobre a Proteção de Dados - GDPR[310], vigente desde maio de 2018. O Regulamento trata da privacidade sobre duas dimensões, tanto da vida privada quanto da liberdade individual, e reconhece a proteção à privacidade como direito fundamental pautado na dignidade da pessoa humana, proteção, como dito, que vem sendo reclamada pelos estadunidenses.

O consentimento necessário regulamentado na União Europeia é voltado ao tratamento dos dados pessoais onde exige-se a demonstração da finalidade de uso, vedado o compartilhamento sem prévia outorga do titular. Desta feita, o princípio da finalidade adotado pela União Europeia torna-se um desdobramento natural do princípio do consentimento. Ademais, os dados sensíveis, assim mencionado na legislação, possuem restrições de compartilhamento, notadamente para fins de evitar discriminações que violam sobremaneira a dignidade da pessoa humana, princípio no qual está inserida a privacidade. Daí podemos extrair as lições de Rodotà[311] ao afirmar:

> Essas preocupações, por exemplo, estão presentes na diretiva Européia 95/46, cujo objetivo declarado é o de oferecer aos cidadãos da União Europeia um elevado nível de tutela dos seus dados pessoais. surgiu assim uma área onde a garantia da privacidade é atualmente a mais vigorosa, em relação aos demais países. o resultado pode parecer paradoxal: na região que a "importou", a Europa, a privacidade tem hoje um estatuto jurídico mais forte do que naquele de sua pátria de origem, os Estados Unidos.
> [...] Se examinarmos isso a disciplina dos "dados sensíveis", ao lado daqueles que efetivamente se referem ao direito de ser deixado só (como os relativos à

[309] BIONI, Bruno R.; ZANATTA, Rafael A. F. "Direito e economia política dos dados: um guia introdutório". *In* Sociedade Vigiada: como a invasão da privacidade por grandes corporações e estados autoritários ameaça instaurar uma nova distopia. Editora: Autonomia Literária. 1ª ed. 2020, p. 108.
[310] Veja <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> Acesso em 15/04/2020.
[311] Op. cit. p. 145.

> saúde ou à vida sexual) estão os dados referentes as opiniões políticas ou sindicais, a filiação a partidos políticos ou outras associações ponto esses últimos dados não se destinam a permanecer reservados ou secretos ponto pelo contrário, caracterizam a esfera pública, devem poder ser livremente os postos em público para oferecer a cada um a possibilidade de participar plenamente da vida civil e política ponto se a eles é atribuída uma tutela particularmente forte, é para evitar discriminações ou exclusões ponto o objetivo, portanto, não é o de favorecer a solidam, mas de garantir a igualdade.

Brasil

A dignidade da pessoa humana fundamenta o estado democrático de direito, como elenca o artigo 1º da Constituição Federal Brasileira. De tal sorte que a privacidade, protegida no artigo 5º, X da *lex mater*, como um dos direitos da perrsonalidade, se reveste da característica de direito fundamental e cláusula pétrea. Diante do amplo alcance do direito à privacidade, a Constituição alude duas expressões distintas relacionadas à privacidade: a intimidade e a vida privada, o que confere à proteção de dados caráter de direito fundamental autônomo como defendido pelo professor Guilherme Martins[312]: "A proteção de dados é vista como um direito fundamental autônomo, essencial para o livre desenvolvimento da personalidade humana".

Seguindo a diretiva Européia, o Brasil aprovou em 2018 a Lei Geral de Proteção de Dados - LGPD, Lei 13.709, cuja vigência ocorreu em plena era pandêmica. De acordo com Patrícia Peck[313] o motivo que inspirou o surgimento dessas regulações de proteção de dados está diretamente relacionado ao próprio desenvolvimento do modelo de negócios da economia digital que passou a ter uma dependência muito maior dos fluxos internacionais de base de dados especialmente os relacionados às pessoas, viabilizados pelos avanços tecnológicos e pela globalização.

O que para Grossi[314] traduziu-se no maior desafio da regulação dos dados pessoais, uma vez que a diferença de visão sobre os direitos da personalidade entre os sistemas jurídicos Continental e do *Common Law*, evidencia o hercúleo desafio de normatizar homogeneamente os dados pessoais sem prejudicar o livre fluxo de pessoas e o comércio internacional.

A LGPD, como se extrai do artigo 6º, é orientada por vários princípios, dentre os quais se extrai o princípio da finalidade e da transparência, em especial atenção dada à questão do

---

[312] MARTINS, Guilherme; LONGHI, João. "Impactos positivos da nova lei brasileira de proteção de dados". *In* Portal ANOREG/SP, 28/08/2018, n.p. Disponível em <https://www.anoregsp.org.br/noticias/35261/artigo-impactos-positivos-da-nova-lei-brasileira-de-protecao-de-dados-porguilherme-martins-e-joao-longhi> Acesso em 28/11/2020.

[313] PINHEIRO, Patrícia Peck. "Proteção de Dados Pessoais: Comentários à Lei 13.709/2018". 2ª ed. São Paulo: Saraiva Educação, 2020, p. 17.

[314] GROSSI, Bernardo Menicucci. "O legítimo interesse como base legal para o tratamento de dados pessoais". *In* Lei Geral de Proteção de Dados: Uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial [recurso eletrônico] Org. Bernardo Menicucci Grossi. Porto Alegre/ RS: Editora Fi, 2020, pp. 64-81. P. 66.

tratamento dos dados, adotando assim, a natural correlação com o consentimento do titular. Na legislação brasileira o consentimento é um dos fundamentos legais do tratamento dos dados pessoais com previsão expressa nos artigos. 7, I e 8º da LGPD, definido no art. 5º, XII como: "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".

De acordo com NOGUEIRA e FONSECA[315], no intuito de conferir maior efetividade ao princípio da autodeterminação informativa, fixou a lei que a realização de uma operação de tratamento de dados pessoais – mediante a obtenção de prévio consentimento do titular – deve se pautar na observação de requisitos rigorosos, além de ser utilizada com parcimônia pelos agentes de tratamento, podendo ser considerado nulo o consentimento caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo, ou mesmo caso não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

Insta ressaltar que o Supremo Tribunal Federal, por ocasião da ADI 6.837[316], ratificou a necessidade de justificativa consistente e legítima para tratamento de dados pessoais. A ADI, promovida pelo Conselho Federal da Ordem dos Advogados do Brasil, rechaçava a Medida Provisória 954/2020, que previa o repasse de nossas informações pessoais de empresas de telefonia para o IBGE para fins estatísticos. Vários ministros enfatizaram que tal regramento traduzir-se-ia em violação ao direito de privacidade, uma vez que a medida provisória pontuava a finalidade de forma genérica.

No voto a ministra Rosa Weber afirma que independentemente do seu conteúdo, mutável com a evolução tecnológica e social, no entanto, permanece como denominador comum da privacidade e da autodeterminação o entendimento de que a privacidade somente pode ceder diante de justificativa consistente e legítima. Assim expondo:

> "Tais informações, relacionadas à identificação – efetiva ou potencial – de pessoa natural, configuram dados pessoais e integram, nessa medida, o âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII). Sua manipulação e tratamento, desse modo, hão de observar, sob pena de lesão a esses direitos, os limites delineados pela proteção constitucional. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais.
> [...] Observo que o único dispositivo da MP n. 954/2020 a dispor sobre a finalidade e o modo de utilização dos dados objeto da norma é o § 1º do seu art. 2º. E esse limita-se a enunciar que os dados em questão serão utilizados

[315] Op. cit. p. 25.
[316] Na íntegra <https://migalhas.uol.com.br/arquivos/2020/4/C47A659344BE14_compartilhamento.pdf> Acesso 24/11/2020.

> exclusivamente pela Fundação IBGE para a produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares. Não delimita o objeto da estatística a ser produzida, nem a finalidade específica, tampouco a amplitude. Igualmente não esclarece a necessidade de disponibilização dos dados nem como serão efetivamente utilizados.

Depreende-se, assim, do breve panorama apresentado, que o consentimento do titular dos dados, tradução da autodeterminação informativa, tanto na legislação europeia quanto no sistema brasileiro, exige por parte daquele que se volta ao tratamento desses dados, a demonstração da finalidade adequada de sua utilização. Ademais, no que concerne os dados sensíveis, assim mencionados, possuem restrições de tratamento, notadamente para fins de evitar discriminações que violem sobremaneira a dignidade da pessoa humana princípio no qual está inserida a privacidade.

Dentro desse contexto voltamo-nos a analisar algumas pesquisas e produtos já colocados em circulação, inclusive no Brasil, no intuito de trazermos à reflexão a adequação e compatibilidade da proteção de dados com as inovações vindouras. Mister observar que todas as pesquisas que passaremos a tratar foram desenvolvidas no âmbito da legislação Americana.

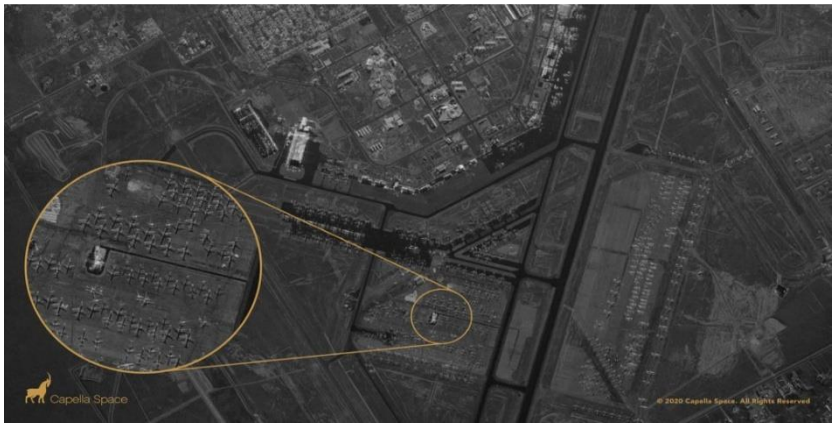
Tecnologias de Monitoramento

O Satélite Capella 2

Nessa aceleração exponencial a empresa norte-americana Capella Space, uma companhia de satélites, lançou neste ano o "Capella 2", um satélite capaz de capturar imagens de alta definição com uma potência surpreendente[317], independentemente de ser dia ou noite. A tecnologia funciona de forma similar ao sistema de ecolocalização usado por golfinhos e

[317] O satélite produz uma onda da região do espectro eletromagnético dentro da faixa que antecede o infravermelho. Tal sinal tem frequência característica de 9,65 GHz, o que significa ter 9 bilhões, seiscentos e cinquenta milhões de oscilações por segundo. Considerando a velocidade de propagação da onda como sendo próxima da velocidade da luz, calcula-se que o sinal tenha comprimento de onda próximo dos 3 centímetros. (Explicação fornecida via contato pessoal por Michael Aleixo dos Santos, doutorando do programa de Pós Graduação em Física Nuclear pelo Instituto Tecnológico de Aeronáutica – ITA). Para obter as imagens o satélite transmite um poderoso sinal de rádio de 9,65 GHz em direção ao seu alvo e, em seguida, coleta e interpreta o sinal conforme ele retorna à órbita. Nessa frequência as nuvens são muito transparentes, o que faz com que se possa enxergar através de fumaça, névoa, umidade e neblina, chova ou faça sol. Veja mais em ROBITZSKI, Dan. "A New Satellite Can Peer Inside Some Buildings, Day or Night". *In* Futurism. Dez/2020. n.p. Disponível em <https://futurism.com/hydra-slime-mold-covid> Acesso em 20/12/2020.

morcegos[318]. Na imagem que segue[319], é possível observar o quanto diferencial é a tecnologia utilizada, uma vez que registra com tamanha nitidez os aviões estacionados no hangar.



Roswell International Air Center, Novo México. Imagens SAR fornecidas pela Capella Space.

As imagens fornecidas[320] impressionam pela nitidez das características demonstradas no espaço geográfico de varredura e, e*mbora seja possível visualizar o interior de algumas estruturas, incluindo a localização de formatos de aviões dentro de hangares, a empresa esclareceu que não é possível ver detalhes dentro de estruturas densas, como arranha-céus ou residências.*

Mas a inovação não fica restrita ao lançamento do satélite e ao seu poder de coleta de imagens. Há previsão do envio de mais outros seis satélites adicionais no ano de 2021. A empresa, recentemente, disponibilizou uma plataforma que permite a qualquer pessoa solicitar imagens definindo o perímetro desejado, como é possível verificar em evento de apresentação feita pela empresa brasileira Visiona Tecnologia Espacial[321] em parceria com a empresa Capella Space.

---

[318] Para aprofundamento no tema veja ARÊDES, Camile; SILVA JUNIOR, Ivo C.; MENDONÇA, Isabela M.; DIAS, Bruno H.; OLIVEIRA, Leonardo W. "Planejamento estático da expansão de sistemas de transmissão de energia elétrica via ecolocalização". Anais do XX Congresso Brasileiro de Automática Belo Horizonte, MG, 20 a 24 de Setembro de 2014. Disponível em <http://www.swge.inf.br/cba2014/anais/PDF/1569926811.pdf> Acesso 14/12/2020.

[319] Imagem apresentada por ROBITZSKI, Dan.op.cit.

[320] A nitidez é tão surpreendente que em uma das imagens mostradas durante apresentação do produto, é possível verificar características das embarcações no porto de Mumbai na Índia e em qualquer outra parte do mundo. As imagens não podem ser divulgadas neste trabalho em virtude de direitos autorais, mas é perfeitamente possível conferir no vídeo de apresentação disponível no canal do Youtube <https://youtu.be/8JtAwjVgpgc> Acesso 14/12/2020.

[321] A Visiona Tecnologia Espacial e a Capella Space, empresa sediada nos Estados Unidos, assinaram recentemente um contrato de distribuição com o objetivo de incorporar ao portfólio da Visiona os dados coletados pelos satélites SAR em banda X operados pela Capella. Maiores informações <https://www.visionaespacial.com.br/sensoriamento-remoto> Acesso em 20/12/2020.

De acordo com Robitzski[322], a resolução das imagens fornecidas poderia vir a ser melhores, uma vez que não há limitações tecnológicas, mas, em virtude da legislação americana, essa seria a melhor resolução possível ao satélite. Dessa forma, contanto que a empresa não melhore a resolução um milímetro além da atual, Banazadeh, CEO da empresa Capella, informou que seus satélites podem capturar imagens de qualquer parte do mundo que um cliente pagante solicitar.

A importância de estabelecimento de limites diante de questões tecnológicas se traduz em questão delicada, mas necessária. Note que a delimitação pautada pela empresa se volta à legislação americana, mas, não se coaduna com a vigilância estabelecida em outras localidades que permeiam o produto posto em comercialização, muito menos aos que dela venham a desfrutar.

Nesse sentido, qual será o limite em relação a privacidade? Qual tratamento será conferido aos dados coletados? Como será definida a finalidade da obtenção de dessas imagens por quem estiver predisposto a pagar o preço (que não é barato)? Uma vez que a empresa coloca uma plataforma a disposição de entidades públicas e privadas, como se fará o controle dos dados que dizem respeito a outras pessoas às quais não foram consultadas e nem sequer podem ter ciência de estarem sendo violadas no seu direito à privacidade?

Nas lições de Rodotà[323]:

> Não devemos jamais nos esquecer que a simples disponibilidade de uma tecnologia não legitima todas as suas utilizações, que devem ser avaliadas com base em valores diferentes daqueles fornecidos pela própria tecnologia. A privacidade não é um obstáculo, porém a via pela qual as inovações científicas e tecnológicas possam legitimamente entrar nas nossas sociedades e nas nossas vidas.

Se a plataforma comercializada com as imagens fornecidas pelo satélite já nos alerta para a questão da privacidade, *p*ermita-nos agora apresentar uma outra tecnologia. E essa, sim, possibilita a obtenção de dados concernentes aos movimentos humanos através da parede.

Tornando o invisível visível: controle de movimentos humanos através de paredes

Pesquisadores do MIT, Instituto de Tecnologia de Massachusetts, universidade privada de pesquisa localizada em Cambridge, desenvolveram um projeto, o "RF-Pose[324]",

---

[322] Idem.
[323] Op. cit. 241.
[324] ZHAO, Mingmin; LI, Tianhong; ALSHEIKH, Mohammad Abu; TIAN, Yonglong; ZHAO, Hang; TORRALBA, Antonio; KATABI, Dina. "Through-Wall Human Pose Estimation Using Radio Signals". *In*

em rede neural profunda[325], no qual a máquina conseguiu extrair movimentos humanos em imagens 2D. O que isto significa? Em termos práticos, implica dizer que a pesquisa demonstrou ser possível estimar movimentos humanos através das paredes em imagens planas[326] (2D), a partir do sinal de wi-fi[327].

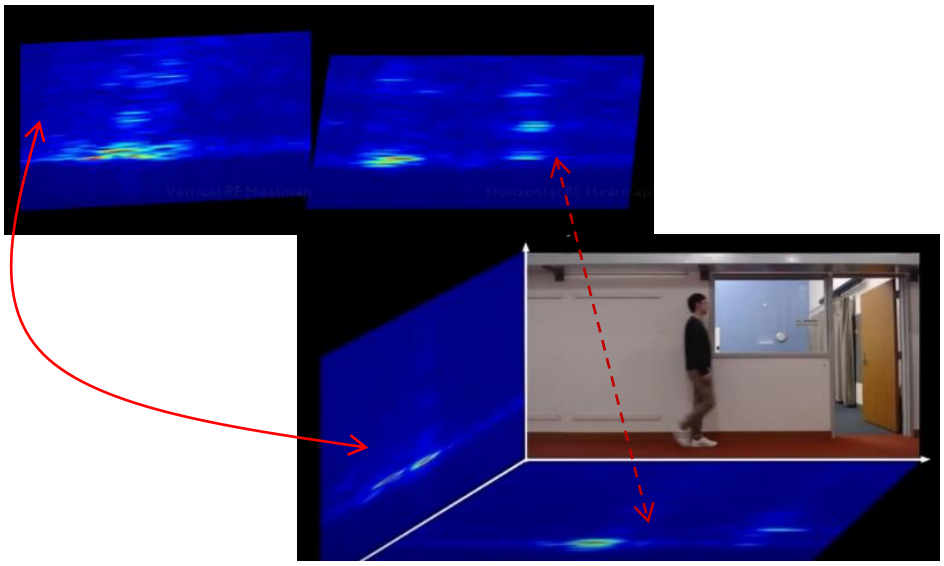
Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Jun/2018. Disponível em <http://rfpose.csail.mit.edu/> Acesso 22/11/2020.

[325] Uma rede neural é um processador maciçamente paralelamente distribuído constituído de unidades de processamento simples, que têm a propensão natural para armazenar conhecimento experimental e torná-lo disponível para o uso. Ela se assemelha ao cérebro em dois aspectos: 1) O conhecimento é adquirido pela rede a partir de seu ambiente através de um processo de aprendizagem; 2) Forças de conexão entre neurônios, conhecidas como pesos sinápticos, são utilizadas para armazenar o conhecimento adquirido. Para aprofundamento HAYKIN, Simon. "Redes Neurais: Princípios e prática". Tradução Paulo Martins Engel. 2ª ed. E-book. São Paulo: Bookman, 2007, p. 28. Disponível em <https://books.google.com.br/books?hl=pt-BR&lr=&id=bhMwDwAAQBAJ&oi=fnd&pg=PP1&dq=redes+neurais+profundas&ots=08quHJMWIq&sig=F57Q0c51wov-tHxd8BVV7Qjc0z4#v=onepage&q=redes%20neurais%20profundas&f=false> Acesso em 14/12/2020. Existem tipos diferentes de redes neurais profundas – e cada um deles possui vantagens e desvantagens, dependendo do uso. Exemplos incluem: Redes neurais convolucionais (RNCs) contêm cinco tipos de camadas: de entradas, de convolução, de agrupamento, as completamente conectadas e as de saída. Cada camada tem um propósito específico, como de resumo, conexão ou ativação. As redes neurais convolucionais popularizaram a classificação de imagens e a detecção de objetos. Entretanto, RNCs também foram aplicadas em outras áreas como previsão e processamento de linguagem natural; Redes neurais recorrente (RNRs) usam informações sequenciais, como dados de registro de data e hora de um sensor ou uma frase dita. Essas informações são compostas por uma sequência de termos. Diferentemente das redes neurais tradicionais, as entradas de uma rede neural recorrente não são independentes umas das outras, e os resultados para cada elemento dependem da computação dos elementos precedentes. RNRs são utilizadas na previsão e aplicação de séries temporais, análise de sentimento e outras aplicações de texto; Redes neurais feedforward, nas quais cada perceptron em uma camada é conectado a todo perceptron da camada seguinte. A informação é entregue de maneira antecipada de uma camada à seguinte seguindo sempre em frente. Não há loops de feedback; Redes neurais autoencoder são utilizadas para criar abstrações chamadas encoders, criados a partir de um conjunto estipulado de entradas. Apesar de similares às redes neurais mais tradicionais, autoencoders procuram modelar as entradas por si só e, portanto, o método é considerado não supervisionado. A premissa dos autoencoders é diminuir a sensibilidade ao que é irrelevante e aumentar ao que é. Conforme camadas são adicionadas, outras abstrações são formuladas em camadas mais altas (camadas mais próximas ao ponto onde uma camada decodificadora é introduzida). Essas abstrações podem, então, ser usadas por classificadores lineares ou não lineares (SAS Insights disponível em <https://www.sas.com/pt_br/insights/analytics/what-is-artificial-intelligence.html> Acesso 14/11/2020).

[326] Para aprofundamento ANDALÓ, Flávio. "Modelagem e animação 2D e 3D para jogos". 1ª Ed. São Paulo: Érica, 2015.

[327] A chamada rede Wi-Fi é uma rede sem fio (também chamada de *wireless*) na qual podemos ter acesso à internet apenas por sinal de ondas de rádio, assim como as televisões e os celulares, não sendo necessária a utilização de fios conectores. As ondas de rádio são ondas eletromagnéticas (formadas pela combinação dos campos elétrico e magnético que se propagam no espaço perpendicularmente transportando energia) utilizadas pelas emissoras de rádio. Basicamente, nos locais onde há sistemas que fazem uso de ondas de rádio, um circuito elétrico é o responsável por provocar a oscilação de elétrons na antena emissora. Estes elétrons são acelerados e, em virtude disso, emitem ondas de rádio, as quais transportam as informações até uma antena receptora. (PIXININE, Juliana. "Como um Wi-Fi funciona? Entenda a tecnologia". *In* TechTudo, 21/02/2015, n.p. Disponível em <https://www.techtudo.com.br/noticias/noticia/2015/02/como-um-wi-fi-funciona-entenda-tecnologia.html> Acesso em 14/12/2020.

Ao contrário da luz visível, o sinal que o roteador envia consegue atravessar paredes. Os pesquisadores criaram um equipamento que emite um sinal na frequência do wi-fi e consegue capturar o reflexo desse sinal pelo ambiente. Utilizado dois planos para capturar o reflexo, um deles paralelo ao chão e o outro perpendicular como demonstrado na imagem.



Imagens coletadas do vídeo de apresentação

Ao capturar o sinal, a informação obtida são manchas imperceptível de identificação de padrão ao olhar humano. Mas, por se tratar de ondas de rádio (as mesmas mencionadas quando tratamos dos satélites), possuem um comportamento definido pelas leis da física. E nesse momento, é que a IA se torna tão importante, uma vez que passa a ser o objetivo da rede neural encontrar a lógica, os padrões. Os dados coletados pelos dois planos são levados para rede neural e ela devolverá um resultado.

Toda rede neural precisa ser treinada. Ela necessita de grandes quantidades de poder computacional e dados. Enquanto os dados treinam o programa para reconhecer padrões, o poder computacional permite que o programa análise esses exemplos em alta velocidade[328]. Atualmente o número de redes neurais especializada em reconhecimento são bem variadas, e uma dessas especializações são as redes neurais "Multi-Person Pose Estimation"[329], capaz de reconhecer a pose de uma pessoa a partir de uma imagem (foto ou vídeo) e criar espécies de bonecos em palitos independentemente de haver sensores na pessoa, como mostra a figura abaixo.

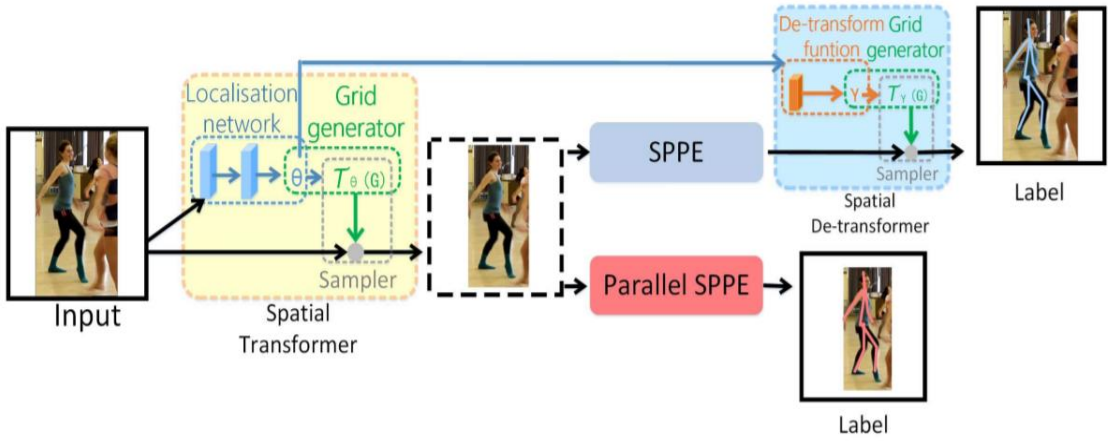


Imagem extraída do artigo FANG, Hao-Shu [*et.al*]. RMPE: Regional Multi-Person Pose Estimation

A utilização desse algoritmo demonstrado na figura foi crucial para o desenvolvimento da pesquisa ora mencionada. Na hora de treinar a rede neural, e como no aprendizado supervisionado você precisa dar a resposta certa para que ela consiga extrair o padrão, eles utilizaram o algorítmo *multi-person* como gabarito para treinar a outra rede neural (*RF-Posed*) que utiliza apenas o reflexo *wi-fi*, ou seja, eles colocaram uma rede neural para supervisionar a outra rede neural. E o resultado apresentado foi a detecção dos movimentos humanos através da parede como demonstra a figura abaixo.

[328] LEE, Kai-Fu. Op. cit. p. 22.
[329] FANG, Hao-Shu; XIE, Shuqin; TAI, Yu-Wing; LU, Cewu. "RMPE: Regional Multi-Person Pose Estimation". *In* The IEEE International Conference on Computer Vision (ICCV), Oct 2017. Disponível em <https://openaccess.thecvf.com/content_ICCV_2017/papers/Fang_RMPE_Regional_Multi-Person_ICCV_2017_paper.pdf> Acesso em 14/12/2020.

Imagem extraída do artigo ZHAO, Mingmin [*et.al*] Through-Wall Human Pose Estimation Using Radio Signals.

Mas isso não é tudo. O artigo apresentado aponta que os dados coletados conseguiram incorporar características na forma de andar que identificam as pessoas. Eles realizaram um experimento com 100 pessoas andando livremente e treinaram uma rede neural convolucional[330] para identificar as pessoas utilizando um vídeo de apenas dois segundos da imagem coletada, observando a forma como o "desenho" se movia. A rede neural conseguiu identificar a pessoa com uma precisão acima de 83% de acurácia. Tanto nos casos em que a pessoa estava visível, quanto nos casos em que a pessoa estava atrás da parede[331].

Apesar de bastante inovador, os pesquisadores não pararam por aí. Na busca de saber quão rica seria a descrição das pessoas[332] que se poderia extrair dos sinais de rádio ao redor, eles avançaram e melhoraram a pesquisa incluindo a obtenção dos movimentos em imagens 3D[333], apresentando o projeto "RF-Pose 3D" [334] e o projeto. Para tanto utilizaram um conjunto de dados abrangendo vários ambientes que incluíam várias pessoas, o que permitiu que o sistema aprendesse a generalizar ambientes não vistos durante o treinamento.

Insta salientar que antes de desenvolverem o projeto ora apresentado, os mesmos pesquisadores, no ano de 2016, apresentaram um projeto capaz de detectar as emoções de uma

---

[330] Vide explicação nota n. 13.

[331] "*We also show that the skeleton learned from RF signals extracts identifying features of the people and their style of moving. We run an experiment where we have 100 people perform free walking, and train a vanilla-CNN classifier to identify each person using a 2-second clip of the RF-based skeleton. By simply observing how the RF-based skeleton moves, the classifier can identify the person with an accuracy over 83% in both visible and through wall scenarios*". ZHAO, Mingmin [et. al] Op. cit. p.7357.

[332] E nessa linha em 2016 foi apresentado pelo mesmo grupo de pesquisa o projeto EQ-Radio capaz de inferir as emoções de uma pessoa usando sinais sem fio. Veja em ZHAO, Mingmin; ADIB, Fadel; KATABI, Dina. "Emotion Recognition using Wireless Signals". *In* MobiCom '16: Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking, October 2016 Pages 95–108. Disponível em <http://eqradio.csail.mit.edu/> Acesso 14/12/2020.

[333] Sobre imagens 3D Vide indicação nota n. 14.

[334] ZHAO, Mingmin; TIAN, Yonglong; ZHAO, Hang; ALSHEIKH, Mohammad Abu; LI, Tianhong; HRISTOV, Rumen; KABELAC, Zachary; KATABI, Dina; TORRALBA, Antonio. "RF-based 3D skeletons". *In* SIGCOMM '18: Proceedings of the 2018 Conference of the ACM Special Interest Group on Data CommunicationAugust 2018 Pages 267–281. Disponível em <https://dl.acm.org/doi/10.1145/3230543.3230579> Acesso 22/11/2020.

pessoa a partir do sinal sem fio. O projeto funciona transmitindo um sinal de radiofrequência e, a partir da análise dos reflexos no corpo de uma pessoa, reconhece o seu estado emocional[335].

Ao medir mudanças sutis na respiração e no ritmo cardíaco o projeto é 87% preciso em detectar se uma pessoa está excitada, feliz ou triste. Dois pontos chamam a atenção: o fato de não ser necessário nenhum tipo de sensor no corpo para fins de detecção das emoções e, por ser apontada, dentre outras, como uma das finalidades para utilização da tecnologia, a possibilidade de análise do comportamento do consumidor.

Entre 2012 a 2019 a equipe de pesquisa, mantendo uma acurácia superior a 80%, conseguiu não apenas monitorar movimentos humanos através das paredes como definir a qual humano pertenceria os movimentos e, ainda, quais as emoções sentidas por um humano não restando a parede como óbice para o resultado.

Não há como negar o impacto e a importância de tal ferramenta para algumas ocorrências do cotidiano e até mesmo para o universo jurídico se pensarmos em produção de provas. Entretanto, por outro lado, também não podemos negar o quanto viola a nossa liberdade, nossa privacidade e o direito fundamental à dignidade.

A identificação das emoções é facilmente observada no vídeo de demonstração disponível na rede [336] e o quanto essa tecnologia pode modificar o mercado, inclusive consumerista. Uma vez que as emoções dos consumidores, frente a produtos ou serviços, possam ser facilmente coletadas (basta pensar no supermercado do futuro inaugurado pela Amazon), também o serão tratadas e, cada vez mais as regras de mercado definirão nossas condutas.

Os mecanismos de controle estão aptos para as tecnologias que estão sendo delineadas?

No ano de 2013 o mundo se surpreendeu com as revelações de Eduard Snowden[337]. Todos éramos vítimas da vigilância massiva dos Estados Unidos, pouco importando se tínhamos ou não algo a esconder.

Como se observou no capítulo anterior, as tecnologias desenvolvidas no MIT avançaram sobremaneira com a utilização de redes neurais. A dimensão de alcance dessas tecnologias é

---

[335] É possível conhecer mais detalhes do projeto através do site do Laboratório de ciência da computação e inteligência artificial do MIT – CSAIL Disponível em <https://www.csail.mit.edu/research/eq-radio-emotion-recognition-using-wireless-signals>. Acesso 18/11/2020.

[336] Para conhecer o projeto e demonstração visual acesse <http://eqradio.csail.mit.edu/>. Acesso 18/11/2020.

[337] *Veja Entrevista concedida pelo ex-agente da NSA* ***Edward Snowden****, que divulgou documentos sobre a espionagem feita pelo governo americano, à jornalista* ***Sonia Bridi****, para o programa Milênio, da GloboNews. 13/06/2014. Disponível em <https://www.conjur.com.br/2014-jun-13/edward-snowden-ainda-revelacoes-serem-feitas-brasil> Acesso 14/12/2020.*

inimaginável e a possibilidade de identificação de movimentos humanos com a possibilidade de identificação através da parede comprova isso. Ainda que se possa ter em mente o benefício do uso para identificação de vítimas em deslizamentos/terremotos, ou o socorro a idosos que residem sozinhos, é preciso refletir sobre o fato de não haver nenhuma regulamentação que delimite o uso de dita tecnologia.

Como vimos o consentimento e a finalidade adequada são basilares da proteção em torno da privacidade, em outras palavras, a autodeterminação informativa impõem que o titular do dado consinta com o seu tratamento. Mas como consentir quando sequer há o conhecimento da coleta de seus dados? O papel da autoridade de proteção de dados ganha novos contornos quando o olhar rompe fronteiras e se desloca para o futuro. Essas inovações tecnológicas estão sendo desenvolvidas sem que qualquer auditoria prévia ou análise de impacto sejam realizadas, implicando dizer que o seu impacto na sociedade tenda a gerar conflitos que nem mesmo podemos vislumbrar em grau de hipótese.

Inobstante a identificação do humano através da parede, também se verifica a possibilidade de identificação de emoções pelo sinal de Wi-Fi. Perceba que a base utilizada para o desenvolvimento do algoritmo foi a mesma em relação a identificação através da parede. Vale dizer que o sinal de Wi-Fi se encontra basicamente em quase todo território mundial, o que nos torna desnudos, vulneráveis diante do alcance desta tecnologia.

Ademais, não se sabe se ela já foi ou está em vias de ser comercializada, ou mesmo se ainda é mantida apenas no laboratório de pesquisa. Nesse sentido a quem caberia ter acesso a dita tecnologia? Como seriam essas imagens armazenadas? Não podemos ignorar o fato de que não há qualquer regramento para aquisição desses produtos e, um crime só é punido quando se consegue descobrir.

Se não é possível confirmar a comercialização da tecnologia baseada em Wi-Fi, por outro lado, a plataforma concernente a obtenção de imagens em alta definição produzida pelo satélite “Capela 2” não só já está sendo comercializada como se encontra disponível no território nacional a partir da parceria feita pela empresa Visiona Tecnologia Espacial.

Mais uma vez a delimitação não é verificada (ao menos não restou mencionada no site da empresa, tampouco na apresentação do produto) em relação ao seu adquirente. O acesso obtido por quem adquirir a plataforma é revestido de opacidade, já que não é possível ter a dimensão de quais informações estão sendo adquiridas através das imagens coletadas, quer seja por entidades governamentais, quer seja pela esfera privada. Duas observações merecem ser trazidas à reflexão.

Primeiro, a ruptura gigantesca de fronteiras em relação à aquisição de imagens, uma vez que estamos lidando com satélite passível de rastrear todo o globo terrestre. Ainda que atualmente o faça num intervalo médio de 4 a 5 horas, muito em breve esse intervalo será reduzido a praticamente 1 hora, tendo em vista que a empresa lançará mais seis satélites voltados à coleta de imagens para aqueles que estiverem dispostos a pagar.

Segundo, e talvez mais preocupante, é comum a reunião de algoritmos para fins de se alcançar um melhor resultado. Nesse sentido, foi demonstrado, que o próprio modelo de inteligência artificial voltado para a identificação de movimentos através da parede, operou a partir do treinamento de um outro algoritmo. A ausência de fiscalização e limite, ou mesmo de análise de impacto desses modelos desenvolvidos com inteligência artificial, nos permite pensar na possibilidade, ainda que possa parecer remota, da reunião dos algoritmos do satélite "Capela 2" com o RF-Posed 3D.

O que se vê no mundo é um total assombro com o alcance da inteligência artificial, isto porque ela está nos levando a lugares nunca imaginados. Tanto a nossa legislação quanto a da União Europeia e mesmo dos Estados Unidos, atuam no contexto do que já conhecemos. É preciso, porém, entender que no âmbito tecnológico os desafios são projetados para uma era cada vez mais futurista, de forma a tornar necessário remodelar o direito para fins de pensarmos na prevenção de certas violações que uma vez ocorridas, talvez não consigamos retornar ao *status quo*.

A amplitude do alcance da privacidade que denota uma dificuldade de definir o campo de proteção, deve permitir, ao menos, que nossa legislação se volte para um regramento no sentido de coibir possíveis violações. Tal qual ocorre com a obrigatoriedade do estudo de impacto ambiental voltados à avaliação dos impactos ambientais[338] que serão gerados pelo empreendimento ou atividade, há que se olhar o quanto antes para o desenvolvimento de um regramento a permitir a análise do impacto tecnológico operado pela inteligência artificial.

Estamos sendo monitorados a cada instante, até mesmo a partir de palavras soltas em redes sociais para fins de analisar a possibilidade de identificação de distúrbios psiquiátricos como demonstra a pesquisa de *Neguine Rezaii* já demonstrada. O que seria feito com a informação que definisse a propensão de doença psiquiátrica em pessoas que estivessem vivendo normalmente? Alterações genéticas? Quais os objetivos pretendem ser alcançados com tais pesquisas?

[338] Vide Res. CONAMA 001/86.

Como afirmou Rodotà[339] para as tecnologias da informação e da comunicação também é preciso questionar se tudo que é tecnicamente possível é socialmente e politicamente aceitável eticamente admissível, juridicamente lícito. Ressurge, a imagem de uma ciência bifronte como o Deus Janus, portadora do bem ou do mal de acordo com a vontade de quem é utiliza e dos contextos nos quais é aplicada.

Conclusão

Ter a consciência de que nossos dados são registrados e permanentemente disponíveis tende a nos modificar tanto individualmente, quanto como sociedade. Não podemos, porém, esquecer, que muitas vezes sequer sabemos o que está disponibilizado ou, o que será permanentemente disponibilizado, vez que só teremos consciência da possibilidade de utilização de nossos dados, diante daquilo que supostamente acessarmos. Entretanto, são nossos dados coletados a todo momento, ainda que não saibamos o porquê, nem a qual finalidade servirá. O simples fato de adquirirmos e utilizarmos dos recursos tecnológicos nos colocam fragilizados e sem qualquer controle sobre nossas informações.

Tal qual a torre que servia para vigiar os presos e que não precisava ter efetivamente ninguém vigiando, mas, a mera ideia de ser vigiado já alterava seus comportamentos, na panóptica de Foucault, nossa sociedade transforma-se em sociedade da vigilância pois não sabemos por quem, mas apenas, que estamos sendo vigiados.

As tecnologias avançam sem que as legislações atuais consigam conter, e o debate gira em torno da não limitação das ciências e das pesquisas. Saber como e por quem serão utilizadas é papel que precisamos desempenhar, notadamente porque aquele que detiver certas tecnologias deterá um poder quase totalitário.

Estamos vulneráveis, precipuamente quando o acesso a produtos e serviços gera como pagamento nossas informações. Nossa legislação e notadamente nosso judiciário não é compatível com as diversas tecnologias operadas por inteligência artificial que estão sendo desenvolvidas e colocadas no mercado.

Buscamos demonstrar que na sociedade da informação, somos monitorados, perfilados, manipulados e sem condição de exercer o consentimento livre. O exercício democrático de autodeterminação informativa é vilipendiado não apenas pelo fato de o acesso vincular-se ao fornecimento dos dados, mas, pelo desconhecimento de quem, ou como nossos dados estejam sendo coletados. Qual sociedade queremos? Qual limite deve ser estabelecido? Ao que parece

[339] Op. cit. p. 142.

a ficção dirigida por Tony Scott “Inimigo do Estado” trazia uma grande verdade: a única privacidade que você tem está na sua cabeça.

As inovações tecnológicas operadas por inteligência artificial já demonstraram o quanto podem trazer benefícios para vários seguimentos da vida humana, e que desabroche a ciência responsiva e ética. Mas que se possa, também, definir os impactos a serem acarretados à vida humana. Que sejamos protagonistas de métodos preventivos, que inviabilizem impactos negativos à privacidade que da tecnologia possa advir!

REFERÊNCIAS:

ADAM, D. “Machines can spot mental health issues—if you hand over your personal data”. *In* MIT Technology Review, 13/08/2020, n.p. Disponível em <https://www.technologyreview.com/2020/08/13/1006573/digital-psychiatry-phenotyping-schizophrenia-bipolar-privacy/> Acesso em 20/09/2020.

ANDALÓ, F. “Modelagem e animação 2D e 3D para jogos”. 1ª Ed. São Paulo: Érica, 2015.

ARÊDES, C.; SILVA JUNIOR, I. C.; MENDONÇA, I. M.; DIAS, B. H.; OLIVEIRA, L. W. “Planejamento estático da expansão de sistemas de transmissão de energia elétrica via ecolocalização”. Anais do XX Congresso Brasileiro de Automática Belo Horizonte, MG, 20 a 24 de Setembro de 2014. Disponível em <http://www.swge.inf.br/cba2014/anais/PDF/1569926811.pdf> Acesso 14/12/2020

BIONI, B. R.; ZANATTA, R. A. F. “Direito e economia política dos dados: um guia introdutório”. *In* Sociedade Vigiada: como a invasão da privacidade por grandes corporações e estados autoritários ameaça instaurar uma nova distopia. Editora: Autonomia Literária. 1ª ed. 2020. pp. 102-142

CAPELAS, B.; WOLF, G. “Mercado de startups do Brasil caminha para ter melhor ano da história em 2020”. Estadão. Out/2020. Disponível <https://economia.uol.com.br/noticias/estadao-conteudo/2020/10/26/mercado-de-startups-do-brasil-caminha-para-ter-melhor-ano-da-historia-em-2020.htm?cmpid=copiaecola> Acesso 14/12/2020.

CASTELLS, M. “A galáxia da internet: reflexões sobre a internet os negócios e a sociedade”. Tradução dos pontos Maria Luiza X. de A. Borges. Revisão técnica: Paulo Vaz. Rio de Janeiro: Jorge Zahar Ed., 2003.

CONESA, F. M. “Derecho a la intimidad, informática y Estado de Derecho”. Universidad de Valencia, Valencia, 1984.

DOBOUR, L. “Sociedade Vigiada: como a invasão da privacidade por grandes corporações e estados autoritários ameaça instaurar uma nova distopia”. Editora: Autonomia Literária. 1ª ed. 2020.

DONEDA, D. C. M. “Da privacidade a proteção de dados pessoais: elementos da formação da lei geral de proteção de dados”. 2ª Ed. São Paulo: Thomson Reuters Brasil, 2020.

FANG, H.S.; XIE, S.; TAI, Y.W.; LU, C. “RMPE: Regional Multi-Person Pose Estimation”. In The IEEE International Conference on Computer Vision (ICCV), Oct 2017. Disponível em <https://openaccess.thecvf.com/content_ICCV_2017/papers/Fang_RMPE_Regional_Multi-Person_ICCV_2017_paper.pdf> Acesso em 14/12/2020.

FOUCAULT, M. “Vigiar e Punir: nascimento da prisão”. Tradução: Raquel Ramalhete. Petrópolis: Vozes, 1987.

GROSSI, B. M. “O legítimo interesse como base legal para o tratamento de dados pessoais”. *In* Lei Geral de Proteção de Dados: Uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial [recurso eletrônico] Org. Bernardo Menicucci Grossi. Porto Alegre/ RS: Editora Fi, 2020, pp. 64-81.

HAN, B.C. “O coronavírus de hoje e o mundo de amanhã”. In El País, 20/03/2020, n.p. Disponível em <https://brasil.elpais.com/ideas/2020-03-22/o-coronavirus-de-hoje-e-o-mundo-de-amanha-segundo-o-filosofo-byung-chul-han.html> Acesso em 03/01/2021

HAYKIN, S. “Redes Neurais: Princípios e prática”. Tradução Paulo Martins Engel. 2ª ed. E-book. São Paulo: Bookman, 2007, p. 28. Disponível em <https://books.google.com.br/books?hl=pt-BR&lr=&id=bhMwDwAAQBAJ&oi=fnd&pg=PP1&dq=redes+neurais+profundas&ots=08quHJMWIq&sig=F57Q0c51wov-tHxd8BVV7Qjc0z4#v=onepage&q=redes%20neurais%20profundas&f=false> Acesso em 14/12/2020.

KERR, O. S. “The Case for the Third-Party Doctrine”. *In* Michigan Law Review. Volume 107. Issue 4, 2009. Disponível em <https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1348&context=mlr> Acesso 30/11/2020.

LEE, K.F. “Inteligência artificial: como os robôs estão mudando o mundo, a forma como amamos, nos comunicamos e vivemos”. Tradução Marcelo Barbão. 1ª ed. Rio d Janeiro: Globo livros, 2019. SAS Insights disponível em <https://www.sas.com/pt_br/insights/analytics/what-is-artificial-intelligence.html> Acesso 14/11/2020

MAFRA W. A. “A privacidade como direito fundamental da pessoa humana”. *In* Sociedade Vigiada: como a invasão da privacidade por grandes corporações e estados autoritários ameaça instaurar uma nova distopia. Editora: Autonomia Literária. 1ª ed. 2020, pp. 11-34.

MARTINS, G.; LONGHI, J. “Impactos positivos da nova lei brasileira de proteção de dados”. *In* Portal ANOREG/SP, 28/08/2018, n.p. Disponível em <https://www.anoregsp.org.br/noticias/35261/artigo-impactos-positivos-da-nova-lei-brasileira-de-protecao-de-dados-porguilherme-martins-e-joao-longhi> Acesso em 28/11/2020.

MOTA, R. “Retrospectiva 2020: ano do e-commerce e avanço dos meios de pagamento”. *In* Olhar Digital, 22/12/2020. Disponível em <https://olhardigital.com.br/2020/12/22/retrospectiva-2020/retrospectiva-2020-ano-do-e-commerce-e-avanco-dos-meios-de-pagamento/?gfetch=2020%2F12%2F22%2Fretrospectiva-2020%2Fretrospectiva-2020-ano-do-e-commerce-e-avanco-dos-meios-de-pagamento%2F> Acesso 03/01/2021.

NOGUEIRA, F. A. C. M.; FONSECA, M. L. “O consentimento na Lei Geral de Proteção de Dados: autonomia privada e o consentimento livre, informado, específico e expresso”. *In* Lei Geral de Proteção de Dados: Uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial [recurso eletrônico] Org. Bernardo Menicucci Grossi. Porto Alegre/ RS: Editora Fi, 2020, pp. 15-35.

PINHEIRO, P. P. “Proteção de Dados Pessoais: Comentários à Lei 13.709/2018”. 2ª ed. São Paulo: Saraiva Educação, 2020, p. 17.

PIXININE, J. “Como um Wi-Fi funciona? Entenda a tecnologia”. 2015, n.p. Disponível em <https://www.techtudo.com.br/noticias/noticia/2015/02/como-um-wi-fi-funciona-entenda-tecnologia.html> Acesso em 14/12/2020.

RODOTÁ, S. “A vida na sociedade da vigilância – a privacidade hoje”. Org. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Ed. Renovar, 2008.

ROBITZSKI, D. “A New Satellite Can Peer Inside Some Buildings”. Day or Night. Futurism. Dez/2020. n.p. Disponível em <https://futurism.com/hydra-slime-mold-covid> Acesso em 20/12/2020.

RUARO, R. L.; RODRIGUEZ, D. P. “O direito à proteção de dados pessoais na sociedade da informação”. *In* Revista Direito, Estado e Sociedade. Programa de Pós-Graduação em Direito da PUC-Rio. n. 36, Jan/Jun2010, pp. 178-199, p. 179). Disponível em <https://revistades.jur.puc-rio.br/index.php/revistades/issue/view/22> Acesso 06/11/2020

RUSSELL, S. J.; NORVIG, P. “Inteligência artificial”. tradução Regina Célia Simille. – Rio de Janeiro: Elsevier, 2013.

SANTANA, W. “Nos EUA, 87% consideram a privacidade de dados como um direito humano”. *In* Olhar Digital, 07/08/2020, n.p. Disponível em <https://olhardigital.com.br/2020/08/07/noticias/nos-eua-87-consideram-a-privacidade-de-dados-como-um-direito-humano/> Acesso 04/12/2020.

SCHNEIER, B. “Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World”. 1ª ed. W. W. Norton & Company, 2015, Ebook Kindle Amazon, cap. 10, n.p.

STAIR, R. M.; REYNOLDS, G. W. “Princípios de sistemas de informação”. 3ª ed. Tradução da 11ª ed. Norte-Americana. Tradução: Noveritis do Brasil. Revisão Técnica: Tânia Fátima Calvi Tait. Editora: Cengage Learning; 2015.

STERN, S. “The Third-Party Doctrine and the Third Person”. *In* New Criminal Law Review, vol. 16, 2013. pp. 101-147. Disponível em < https://tspace.library.utoronto.ca/bitstream/1807/87908/1/Stern%20Third%20Party%20Doctrine.pdf> Acesso 30/11/2020.

THOMPSON II, R. M. “The Fourth Amendment Third-Party Doctrine”. *In* Congressional Research Service. 2014. Disponível em < https://fas.org/sgp/crs/misc/R43586.pdf> Acesso 30/11/2020.

WARREN, S. D.; BRANDEIS, L. D. “The Right to Privacy”. *In* Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220, p. 195. Disponível em <https://www.jstor.org/stable/1321160?seq=1#metadata_info_tab_contents> Acesso 08/08/2020.

ZANINI, L. E. A. “O surgimento e o desenvolvimento do *right to privacy* nos Estados Unidos”. *In* Revista Jus Navigandi, Teresina, ano 22, n. 5130, 18/07/2017. Disponível em <https://jus.com.br/artigos/57228> Acesso 04/01/2020.

ZHAO, M.; ADIB, F.; KATABI, D. “Emotion Recognition using Wireless Signals”. MobiCom '16: Proceedings of the 22nd Annual International Conference on Mobile Computing and NetworkingOctober 2016 Pages 95–108. Disponível em <http://eqradio.csail.mit.edu/> Acesso 14/12/2020.

ZHAO, M.; LI, T.; ALSHEIKH, M. A.; TIAN, Y.; ZHAO, H.; TORRALBA, A.; KATABI, D. “Through-Wall Human Pose Estimation Using Radio Signals”. *In* Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Jun/2018. Disponível em <http://rfpose.csail.mit.edu/> Acesso 22/11/2020.

ZHAO, M.; TIAN, Y; ZHAO, H.; ALSHEIKH, M. A.; LI, T.; HRISTOV, R.; KABELAC, Z.; KATABI, D; TORRALBA, A. “RF-based 3D skeletons” SIGCOMM '18: Proceedings of the 2018 Conference of the ACM Special Interest Group on Data CommunicationAugust 2018. Pages 267–281. Disponível em <https://dl.acm.org/doi/10.1145/3230543.3230579> Acesso 22/11/2020.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS: FORMAÇÃO, AUTONOMIA E LEGITIMIDADE

Pedro Henrique de Paula Morais
Marcos Cesar de Souza Lima

INTRODUÇÃO

Na reflexão de Adorno e Horkheimer, com a instalação da modernidade, o indivíduo se colocou no centro de todas as reflexões, passando a acreditar que o esclarecimento o tornaria senhor de suas ações, e que a racionalidade o libertaria de qualquer violência a liberdade. Todavia, é este avanço da técnica sobre a natureza que acaba por estabelecer a dominação do homem sobre o próprio homem, retirando-lhes sua capacidade como indivíduo singular, tornando-o parte de uma massa[340].

Assim, com a entrada do século XX, abandonaram-se as utopias positivas, adotando-se um discurso pautado no temor as transformações advindas da tecnologia. "Mas a angústia do futuro não implica a recusa do futuro"[341], de modo que cabe aos indivíduos e aos grupos controladores, dessas novas e inarredáveis ferramentas de transformações ligadas à internet, utilizar-se delas não só como um meio de garantir um poder legítimo, mas também de expandir as liberdades individuais, como nunca antes feito[342].

Manuel Castells sustenta que "se a primeira revolução industrial foi britânica, a primeira revolução tecnológica da informação foi norte-americana"[343], ocorreu principalmente no Vale no Silício a partir da década de 70, e com o aprimoramento da capacidade de comunicação da rede, gerou um crescimento exponencial no volume de informação e dados[344]. A partir desta revolução, gerou-se mais informação do que em toda a história humana anterior, a capacidade de gerar, armazenar e transmitir dados[345], mudou o modo dos indivíduos interagirem, das

---

[340] ADORNO, Theodor. **Dialética do esclarecimento**, Editora Schwarcz-Companhia das Letras, 1947, p.111 a 116. Disponível em: <https://files.cercomp.ufg.br/weby/up/208/o/fil_dialetica_esclarec.pdf>. Acesso em 02 de Agosto de 2020.
[341] RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008, p.39.
[342] RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008, p.24.
[343] CASTELLS, Manuel, **A sociedade em Rede**. v.1, 8ª ed., Tradução de Roneide Venancio Majer, São Paulo: Editora Paz e terra, 2005, p.99.
[344] CASTELLS, Manuel, **A sociedade em Rede**. v.1, 8ª ed., Tradução de Roneide Venancio Majer, São Paulo: Editora Paz e terra, 2005, p.84-90.
[345] Conforme Bruno Bioni, "O dado é o estado primitivo da informação, pois não é algo per se que acresce conhecimento. Dados são simplesmente fatos brutos que, quando processados e organizados, se convertem em algo inteligível, podendo ser deles extraída uma informação". BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Forense, 2019, p.54.

sociedades empresárias buscarem o lucro, e dos Estados garantirem sua soberania[346].“Dados são o novo petróleo, a diferença é que o petróleo vai acabar um dia. Os dados, não”[347], afirmou Ajay Banga, CEO da Mastercard, durante o Master Minds em 2019.

Neste cenário, os bancos de dados se tornaram uma constante, crescente e valiosa, passando os indivíduos a serem identificados pelas informações coletadas, sejam por agentes públicos ou privados[348]. Com o aprimoramento da técnica, fez-se destas informações um ativo econômico, social e político, capaz de aumentar lucros de grandes corporações, de influenciar eleições, e de diagnosticar problemas e soluções sociais[349].

Deste modo, “as informações coletadas, além de fazer as organizações públicas e privadas capazes de planejar e executar seus programas, ainda permitem o surgimento de novas concentrações de poder ou o fortalecimento de poderes já existentes”[350]. Portanto, se o processamento de dados é fator condicionante a modificação da estrutura social, a maneira como o utilizamos e regulamos, é determinante na construção da sociedade de informação[351].

Em 1980, foi publicado o artigo “*The Right to Privacy*”, de Samuel Warren e Lois D. Brandeis, texto que inaugura a reflexão sobre a necessidade de criar instrumentos jurídicos capazes de garantir a privacidade nesta nova era digital[352]. No mesmo ano da publicação, a OCDE emitiu o “*Privacy Guidelines”*, e cinco anos mais tarde a “*Declaration on Transborder Data Flows”,* criando metas e diretrizes para a proteção global de dados pessoais[353].

Deste momento em diante, expandiu-se a discussão por todo o globo sobre a matéria, passando os tribunais constitucionais a tratarem da matéria de forma específica, como ocorreu em 1983, na Alemanha, ao definir a corte o direito à autodeterminação informativa, como “o

---

[346] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p.5-16.
[347] ÉPOCA NEGÓCIOS. “**Dados são o novo petróleo**” dix CEO da Mastercar. 05 de Julho de 2019. Disponível em: <https://epocanegocios.globo.com/Empresa/noticia/2019/07/dados-sao-o-novo-petroleo-diz-ceo-da-mastercard.html>. Acesso em: 07 de Agosto de 2020.
[348] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p.7-8.
[349] RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008, p.28-32.
[350] RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008, p.37.
[351] LÉVY, Pierre. **Cibercultura**, Tradução de Carlos Irineu Costa. Editora 34, 2010. p. 123-125. Disponível em: <https://mundonativodigital.files.wordpress.com/2016/03/cibercultura-pierre-levy.pdf>. Acesso em 05 de Agosto de 2020.
[352] WARREN, Samuel D.; BRANDEIS, Louis D. **The right to privacy**. Harvard law review, v. 4, n. 5, p. 193-220, 1890. Disponível em: <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>. Acesso em 10 de Agosto de 2020.
[353] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Forense, 2019, p.118.

direito de os indivíduos decidirem por si próprios quando e dentro de quais limites seus dados pessoais poderão ser utilizados"[354]

Adotou-se ainda no período, a Convenção nº108/1981 (Convenção de Stransbourg), responsável pela criação da Primeira Autoridade responsável pela proteção dos dados pessoais, e, após ela, passou-se a desenvolver em todo o mundo legislações neste sentido.

Nestes modelos robustecidos desde 1980, na busca pela efetivação da garantia a privacidade e a proteção dos dados pessoais, as Autoridades de Proteção de Dados, mostraram-se vitais, tornando-se parte indissociável da "estrutura administrativa e jurídica estatal", e garantido que a legislação seja aplicada dentro de seus limites e fins[355].

Destaque para o modelo europeu de proteção de dados pessoais, que se tornou referência mundial, com a criação das chamadas "autoridades de controlo", que à partir do Protocolo Adicional à Convenção 108, de 2001, tornaram-se obrigatórias nos países membros do Conselho da Europa[356].

Consolidando essa estrutura, no âmbito da União Europeia, as autoridades de controle são desenhadas de maneira clara pelo art. 28 da Diretiva de Proteção de Dados (Diretiva 95/46/CE), que estabelece que: "Essas autoridades exercerão com total independência as funções que lhes forem atribuídas"[357].

A importância destas autoridades foi reafirmada recentemente, em 2018, com a promulgação do moderno Regulamento Geral de Proteção de Dados (GPDR), que entre os artigos 51 a 59 fixa características, finalidades, responsabilidades, atribuições, competências e poderes[358].

O Brasil, dentre as nações integrantes do G20, foi o último país a promulgar uma Legislação específica versando sobre a proteção dos dados pessoais. Somente em 2018 a Lei Geral de Proteção de Dados (Lei 13.709/2018) foi aprovada, tendo sua vigência inicialmente adiada para 03 de maio de 2021 pela MP 959 de 2020, todavia, com a exclusão do adiamento

---

[354] RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. **O direito à proteção de dados pessoais na sociedade da informação**. Revista Direito, Estado e Sociedade, n. 36, 2010, p.191-192. Disponível em: <https://revistades.jur.puc-rio.br/index.php/revistades/article/view/212>. Acesso em 11 de Agosto de 2020.

[355] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p.387.

[356] EUROPEU, CONSELHO. **Manual da Legislação Europeia sobre Proteção de Dados**, 2014, p.123. Disponível em: <https://www.echr.coe.int/Documents/Handbook_data_protection_POR.pdf>. Acesso em: 12 de Agosto de 2020.

[357] EUROPEU, CONSELHO. **Manual da Legislação Europeia sobre Proteção de Dados,** 2014, p.123. Disponível em: <https://www.echr.coe.int/Documents/Handbook_data_protection_POR.pdf>. Acesso em: 12 de Agosto de 2020,p.129.

[358] EUROPEU, CONSELHO. **Manual da Legislação Europeia sobre Proteção de Dados**, 2014. Disponível em: <https://www.echr.coe.int/Documents/Handbook_data_protection_POR.pdf>. Acesso em: 12 de agosto de 2020, p.132.

do texto da MP pelo Senado, entrou em vigor às vésperas do presente estudo, em Agosto de 2020.

Em que pese a Autoridade Nacional de Proteção de Dados (ANPD), ela estava prevista no Projeto de Lei 5.276/2016, que serviu de base para a LGPD aprovada, e foi instituída inicialmente como autarquia especial, com ampla autônima e atribuições que permitam a centralização do poder de proteção dos dados[359].

O projeto caminhava a passos lentos na Câmara, até que em 2018 eclodiu o escândalo da *Cambrigde Analytica*[360], deixando evidente o impacto do uso dos dados pessoais na atual sociedade, e sua capacidade de influenciar o sistema democrático como um todo, colocando em xeque, inclusive, a legitimidade da eleição americana de 2016[361].

Assim, o PL 5.276/2016 foi substituído pelo PLC 53/2018, que instituída em seu art.55 a ANPD como "integrante da administração pública federal indireta, submetido a regime autárquico especial e vinculado ao Ministério da Justiça"[362]. Ao sancionar o projeto, criando então a LGPD, o Presidente Michel Temer, vetou referido dispositivo, alegando vício constitucional na iniciativa, e que a Autoridade não poderia onerar o orçamento do poder do Executivo[363].

Diante do veto, editou-se a MP 869 de 2018, convertida na Lei 13.853/2019, criando finalmente a ANPD, mas agora como órgão da administração pública direta, assegurada a autonomia técnica e decisória, mas não financeira (art.55-A e 55-B).

---

[359] BRASIL. Câmara dos Deputados, Projeto de Lei, **PL 5276/2016**. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>. Acesso em: 10 de agosto de 2020.

[360] "Descobriu-se, outrossim, que a Cambridge se utilizou de conhecimentos teóricos das ciências comportamentais para identificar diversos parâmetros de personalidade existentes na imensa base de dados colhidos e, com isso, engendrou uma campanha publicitária específica para cada tipo de usuário. Umas das bases para o engenho foram as "curtidas" deixadas pelos internautas no Facebook, bem como pesquisas aparentemente sem maiores repercussões, tais como: que animal mais combina com você? Desse modo, 'Trump e sua equipe eleitoral conseguiram montar perfis de personalidade de eleitores potencias de forma mais efi ciente que seus concorrentes'". MARTINS, Marcelo Guerra; TATEOKI, Victor Augusto. **Proteção de dados pessoais e democracia: fake news, manipulação do eleitor e o caso da Cambridge Analytica**. Revista Eletrônica Direito e Sociedade-REDES, v. 7, n. 3, 2019, p.144. Disponível em: <https://revistas.unilasalle.edu.br/index.php/redes/article/view/5610>. Acesso em 12 de Agosto de 2020.

[361] PERSILY, Nathaniel. **The 2016 US Election: Can democracy survive the internet?.** Journal of democracy, v. 28, n. 2, p. 63-76, 2017. Disponível em: <https://research.steinhardt.nyu.edu/scmsAdmin/media/users/jzf206/Persily.pdf.> Acesso em: 10 de Agosto de 2020.

[362] BRASIL. Câmara dos Deputados, Projeto de Lei Complementar, **PLC 53/2018**. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/133486>. Acesso em 10 de Agosto de 2020.

[363] PAULA, Felipe; NAGELE, Vitor Rabelo. **Há vício de iniciativa na criação da Autoridade Nacional de Proteção de Dados?**. JOTA Regulação, 26 de Julho de 2018. Disponível em: <https://www.jota.info/tributos-e-empresas/regulacao/ha-vicio-de-iniciativa-na-criacao-da-autoridade-nacional-de-protecao-de-dados-26072018>. Acesso em 13 de Agosto de 2020.

Assim, com a conversão da MP 959 de 2020 na Lei 14.010/2020, sem o trecho que estendia a vacância da LGPD, foi o governo compelido a editar o Decreto 10.474/20, que cria a estrutura da ANPD, muito embora, conforme fixado no art.65, I-A, da LGPD, alterado pela Lei 14.010/20, as possíveis sanções aplicáveis pela autarquia ficam suspensas até agosto de 2021, esvaziando a importância do órgão até esta data.

1. TECNOLOGIA: DA DOMINAÇÃO À LIBERTAÇÃO

Para melhor compreender o papel da Autoridade Nacional de Proteção de Dados, faz-se necessário utilizar a larga discussão teórica sobre a privacidade e o avanço tecnológico, que tem seu prólogo na reflexão dos efeitos da tecnologia no desenvolvimento social, e avança no desenvolver das autoridades de controle de dados na regulação destes impactos. Nas palavras de Marcuse:

> Hoje, a dominação eterniza-se e amplia-se não só mediante a tecnologia, mas como tecnologia; e esta proporciona a grande legitimação ao pode político expansivo, que assume em si todas as esferas da cultura. Neste universo, a tecnologia proporciona igualmente a grande racionalização da falta de liberdade do homem e demonstra a impossibilidade "técnica" de ser autônomo, de determinar pessoalmente sua vida
> Nesse universo, a tecnologia também garante a grande racionalização da não-liberdade do homem e demonstra a impossibilidade "técnica", de a criatura ser autônomo de determinar a sua própria vida. Isso porque essa não-liberdade não parece irracional nem política, mas antes uma submissão ao aparato técnico que amplia as comodidades da vida e aumenta a produtividade do trabalho. A racionalidade tecnológica protege, assim, em vez de cancelar, a legitimidade da dominação, e o horizonte instrumentalista da razão se abre sobre uma sociedade racionalmente totalitária [364].

Assim, em nossa percepção, embora Herbert Marcuse, acredite que a tecnologia permaneça sendo um meio de dominação à partir da racionalização técnica, existe nela um elemento de libertação, por fazer da técnica meio não apenas de coação, mas também de produção, de maneira que: "A tecnologia serve para instituir formas mais eficazes e mais agradáveis de controle social e coesão social"[365].

Diferente de Marcuse, Habermas não acreditava ser a tecnologia capaz de diminuir o caráter explorador da dominação, tão pouco que há uma nova forma de racionalização intrínseca

---

[364] MARCUSE, Herbert. **A ideologia da sociedade industrial: o homem unidimensional.** 4 ed. Tradução de Giasone Rebuá. Rio de Janeiro: Zahar Editores, 1973, p.154. Disponível em: <https://cesarmangolin.files.wordpress.com/2011/08/marcuse-a_ideologia-da-sociedade-industrial-o-homem-unidimensional.pdf.> Acesso em 16 de Agosto de 2020.
[365] MARCUSE, Herbert. **A ideologia da sociedade industrial: o homem unidimensional.** 4 ed. Tradução de Giasone Rebuá. Rio de Janeiro: Zahar Editores, 1973, p. 174.

nesta nova técnica, capaz de reconciliar homem e natureza[366]. Neste ponto, a visão cética de Habermas parece coincidir com a de Adorno e Horkheimer, na obra "Dialética do Esclarecimento", e a compreensão de que esta racionalidade tecnocientífica, aqui, instrumentalizada pela tecnologia, não seria capaz de emancipar o homem, pelo contrário, o paralisa e o torna impotente[367].

Deste modo, em certa medida, sem abandonar a crítica ao Iluminismo e a racionalidade técnica, Marcuse inaugura uma reflexão menos cética que a defendida por Habermas e demais autores da escola de Frankfurt, quanto a possibilidade de conciliar razão, liberdade e técnica.

> A tecnologia pode, assim, garantir a correção histórica da identificação prematura da Razão e da Liberdade, graças à qual o homem pode tornar-se e permanecer livre no progresso da produtividade autoperpetuadora com base na opressão. No quanto a tecnologia se desenvolveu nessas bases, a correção jamais poderá ser o resultado do progresso técnico per se. Ela compreende uma reversão política[368].

Assumindo a possibilidade de a tecnologia coexistir pacificamente como instrumento não apenas de poder e dominação, mas também de libertação do homem do próprio homem, com potencial político capaz de mudar a exploração fundada numa racionalidade puramente técnica [369], Marcuse abre caminho para o desenvolvimento de teorias que procuram compatibilizar avanço tecnológico, social e democrático, como a realizado por Feenberg.

Passa então, na reflexão de Feenberg, a tecnologia a ser tratada não como um mero instrumento de dominação, mas como fenômeno social autônomo. Deixa de ser mera condição de meio e passa a incorporar valores e culturas, tornando-se ainda, instrumento de deliberação democrática. Neste ponto, Feenberg sinaliza a necessidade de Habermas rever a Teoria da Ação Comunicativa, reconstruindo a análise de modo a considerar a tecnologia não apenas como meio instrumental voltada à dominação[370].

---

[366] HABERMAS, Jurguen. **Técnica e Ciência como "ideologia**". Tradução de Artur Mourão. Edições 70: Lisboa, 1968, p. 49. Disponível em: <http://www.afoiceeomartelo.com.br/posfsa/Autores/Habermas,%20J%C3%BCrgen/T%C3%A9cnica%20e%20ci%C3%AAncia%20como%20ideologia.pdfhttp://www.afoiceeomartelo.com.br/posfsa/Autores/Habermas,%20J%C3%BCrgen/T%C3%A9cnica%20e%20ci%C3%AAncia%20como%20ideologia.pdf>. Acesso em 17 de agosto de 2020.

[367] ADORNO, Theodor. **Dialética do esclarecimento**. Editora Schwarcz-Companhia das Letras: São Paulo, 1947, p.111 a 116. Disponível em: <https://files.cercomp.ufg.br/weby/up/208/o/fil_dialetica_esclarec.pdf>. Acesso em 02 de agosto de 2020.

[368] MARCUSE, Herbert. **A ideologia da sociedade industrial: o homem unidimensional.** 4 ed. Tradução de Giasone Rebuá. Rio de Janeiro: Zahar Editores, 1973, t., p.14.

[369] MARCUSE, Herbert. **Algumas implicações sociais da tecnologia moderna**. In: MARCUSE, Herbert; KELLNER, Douglas (ed.), **Tecnologia, Guerra e Fascismo**. Fundação Editora da Unesp: São Paulo, 1999, p. 71-104.

[370] NEDER, Ricardo T. (org.). **A teoria crítica de Andrew Feenberg. racionalização democrática**, **poder e tecnologia**. Escola de Altos Estudos da Capes: Brasília, p. 205-2020. Disponível em: <https://www.sfu.ca/~andrewf/coletanea.pdf>. Acesso em 18 de agosto de 2020.

Feenberg, em sua crítica a tecnologia, concilia a razão instrumental com o interesse social, sob a defesa que a eficiência trazida pelo avanço tecnológico possibilita a concretização da vontade coletiva, não como fenômeno imutável e inevitável, mas alterável pela vontade política em sua melhor definição[371].

Então, na interseção entre ideologia e técnica, o pensador devolve o que chama de "código técnico", conceituado como:

> Um código técnico é a realização tecnicamente coerente de um interesse numa solução para um tipo geral de problema. Essa solução então serve como um paradigma ou exemplo para todo um domínio da atividade técnica. A noção de código técnico pressupõem que existem muitas soluções diferentes para problemas técnicos[372].

É partindo desta revisão, que se pretende desenvolver o trabalho, esforçando-se para conciliar a racionalidade tecnocientífica, aqui, materializa nos dados pessoais e sua transferência, com o interesse social, ou, neste trabalho, o direito a privacidade.

Sob esta dialética, chega-se ao que Castells chama de sociedade em rede, em que técnica e a vontade política prosperam pelo domínio da informação, que como nunca antes, torna-se protagonista na condução da mudança cultural. Neste sentido, "A emergência de um novo paradigma tecnológico organizado em torno de novas tecnologias da informação, mais flexíveis e poderosas, possibilita que a própria informação se torne o produto do processo produtivo[373].

Neste sentido, Pierre Lévy sustenta que a sociedade de informação é constituída pelo desenvolvimento digital e tecnológico, modificando as estruturas sociais e formando uma cultura digital. Esta nova técnica, ligada as tecnologias, tem sua centralidade não em sua existência em si, mas na maneira como o homem irá desenvolvê-la. Não é a tecnologia um fator autônomo ou separado da sociedade, pelo contrário, está nela inserida de maneira indissociável, por ser impossível afastar o humano de seu ambiente material[374].

Embora a tecnologia influencie na formação da sociedade, não é ela um fator determinante, mas sim condicionante. Deste modo, o que definirá o futuro não é apenas o

---

[371] FEENBER, Andrew. **Questioning Technology**. 3 ed.. Routeledge – Taylor & Francis Group: London and New York, 2001. p.207-209.

[372] FEENBER, Andrew. **Transforming Technology, a critical theory revisited**. Oxford University Press: New York, 2002, p.20-21. Disponível em: <https://monoskop.org/images/d/d8/Feenberg_Andrew_Transforming_Technology_A_Critical_Theory_Revisited.pdf>. Acesso de 15 de Agosto de 2020.

[373] CASTELLS, Manuel, **A sociedade em Rede**. v.1, 8ª ed., Tradução de Roneide Venancio Majer, São Paulo: Editora Paz e terra, 2005, p.119.

[374] LÉVY, Pierre. **Cibercultura**, Tradução de Carlos Irineu Costa. Editora 34, 2010. p. 123-125. Disponível em: <https://mundonativodigital.files.wordpress.com/2016/03/cibercultura-pierre-levy.pdf>. Acesso em 05 de Agosto de 2020, p.19-25.

surgimento e a disseminação de novas tecnologias, mas a forma como o homem irá tratar as novas ferramentas disponíveis[375].

2. A FUNDAMENTAL TUTELA DOS DADOS PESSOAIS E AS AUTORIDADES DE CONTROLE

Assim, neste novo arranjo social, orientado pela tecnologia, e principalmente pela forma como à instrumentalizamos, a informação se torna elemento nuclear, transformando-se em elemento estruturante e balizador da nova sociedade. A informação, e acima de tudo a capacidade de ter acesso a ela, tornou-se sinônimo de riqueza e poder[376].

Passou-se a reconhecer em todo o mundo, a importância de tutelar os dados pessoais, inclusive, tratando a matéria como afeta aos direitos fundamentais. Danilo Doneda registra que a Convenção de Strabourg marca esta abordagem, evidenciando que a proteção de dados pessoais está ligada "à proteção dos direitos humanos e das liberdades fundamentais, entendendo-a como pressuposto do estado democrático e trazendo para este campo a disciplina"[377].

Laura Shertel, na mesma linha, utilizando-se da experiência estrangeira, defende que a tutela jurídica dos dados pessoais, em âmbito nacional, deve ser efetivada à partir de uma racionalidade que proteja não o dado em si, mas sim seu titular, conferindo a essa proteção a posição de direito fundamental, e, por consequência, impondo ao Estado o dever de regulá-la de maneira mais próxima[378].

Com a evolução da capacidade de tecnológica, e a constituição de uma sociedade em rede[379], ficou clara a necessidade de tutelar de maneira efetiva estes dados, ligados intimamente com a nova compreensão de privacidade, que, segundo Rodotà seria "o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular"[380],

---

[375] LÉVY, Pierre. **Cibercultura**, Tradução de Carlos Irineu Costa. Editora 34, 2010. p. 123-125. Disponível em: <https://mundonativodigital.files.wordpress.com/2016/03/cibercultura-pierre-levy.pdf>. Acesso em 05 de Agosto de 2020, p. 26-30.

[376] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Forense, 2019, p.19-22.

[377] DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico Journal of Law [EJJL], v. 12, n. 2, 2011, p.101-102. Disponível em: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315>. Acesso em: 10 de Agosto de 2020.

[378] MENDES, Laura Scherthel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fudamental**, Saraiva: São Paulo, 2014, p.78-80.

[379] CASTELLS, Manuel, **A sociedade em Rede**. v.1, 8ª ed., Tradução de Roneide Venancio Majer, São Paulo: Editora Paz e terra, 2005, p.98-99.

[380] RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008, p.15.

Na busca pela consolidação deste direito a proteção de dados, instituiu-se as Autoridades de controle[381], que na Europa foram constituídas na forma Autoridades Administrativas independentes, que, segundo Michel Gentot são:

> Para definir as autoridades administrativas independentes, pode-se dizer que essas são as comissões que têm um poder de regulação autônomo na área em que são chamadas a agir. As áreas de intervenção são: ciência da computação, comunicação audiovisual, administração, mercado, mercado de ações e consumo. Como se pode ver, esses são setores sensíveis da vida econômica e social de um país, para os quais é importante estabelecer uma grande medida de liberdade em paralelo com o controle estatal que não pode ser exercido diretamente. O papel da regulação é assim atribuído a essas instâncias[382] (tradução livre).

Por conseguinte, as Autoridades de Proteção de Dados (DPA), constituem importante instrumento do Estado Regulador Europeu, que busca no afastamento da atuação direta na economia, melhorar a eficiência e a capacidade de governança do Estado, fazendo com que atuem não apenas controlador do fluxo de dados, mas também como agente capaz de introduzir mudanças de comportamento, garantido não só a proteção de dados, mais a privacidade dos usuários[383].

Mesmo com um sistema consolidado, há na doutrina europeia, profunda discussão sobre a autonomia das Autoridades de Controle, a independência de seus membros, e a legitimidade de sua atuação.

A independência das DPA varia de acordo com o país analisado, apesar da Diretiva 95/46/EC ter gerado certa uniformização, fazendo com que ocorra no continente contínuo diálogo entre os organismos, no escopo de analisar se a atuação é satisfatória, sob o prisma da Diretiva. Como exemplo, cita-se a obra "*European Data protection: In Good Health*?"[384].

A independência dos dirigentes, de igual maneira, tem gerado debates, principalmente após o caso Alemão, país com tradição na regulação de dados, desde 1978, e que serviu, inclusive, como modelo para a formação do regime de proteção de dados da U.E.

---

[381] RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008, p.199.

[382] GENTOT, Michel. **Les Autorites Administratives Independantes**. Universite Claude Bernard Lyon I: Conseil d' etat, 1991, p.4. Disponível em: <https://www.enssib.fr/bibliotheque-numerique/documents/62448-lesautorites-administratives-independantes.pdf>. Acesso em 14 de Agosto de 2020.

[383] BENNET. Colin J., **Regulatory Privacy, Data protection and Public Policy in Europe and the United Stades**, Cornell Universty Press: Ithaca and London, 1992, p.135. Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=&id=D17pcdORb9UC&oi=fnd&pg=PR7&dq=+europe+data+protection+authority+features&ots=ityrRuErij&sig=s2q6vaEVYnOI24RkQl5AQ5hG3DM&redir_esc=y#v=onepage&q&f=false>. Acesso em 18 de Agosto de 2020.

[384] GUTWIRTH, Serge; LEENES, Ronald; DE HERT, Paul; POULLET, Yves, **European Data Protection: In Good Health?**. Springer: London and New York, 2012. Disponível em <https://link.springer.com/content/pdf/10.1007%2F978-94-007-2903-2.pdf>. Acesso em 17 de Agosto de 2020.

No país, o responsável pela tutela dos dados e garantia da privacidade é o Comissário Federal para proteção de dados e liberdade de informação (FfDf), vinculado diretamente ao Ministério Federal do Interior, possui ainda autoridades com atuação regionais, ligadas aos governos locais.

A estreita ligação entre o governo e as autoridades de controle, fez com que a Agência Europeia de Proteção de Dados, ingressasse com ação em face da República Alemã, alegando violação do princípio da total independência, previsto no art. 28, 1, §2º da Diretiva 95/46/EC. A Corte Europeia de Justiça (ECJ) verificou que, de fato, as autoridades careciam de independência funcional, na medida em que os funcionários estavam sendo influenciados pelo Ministério do interior, que detinha gerência sobre suas carreiras públicas[385].

O amadurecimento da reflexão no Continente Europeu, fez gerar discussões que ultrapassam o questionamento sobre a eficiência e independências das Autoridades de Controle, passando-se assim, sob influência da literatura do professor Giandomenico Majone, e sua crítica sobre a défcit democrática na atuação regulatória de entes não eleitos[386], a se discutir também sua legitimidade.

No Brasil, ainda é incipiente o estudo sobre autoridades de controle de dados, o que se justifica pelo atraso legislativo, que veio a criar a ANPD somente em 2019. Todavia, já é reconhecida pela doutrina, aqui representada por Danilo Doneda, expoente literato no estudo da proteção de dados no país, a importância e necessidade do organismo:

> Outra característica é a disseminação do modelo das autoridades independentes para a atuação da lei – tanto mais necessária com a diminuição do poder de "barganha" com o indivíduo para a autorização ao processamento de seus dados, e também o surgimento de normativas conexas na forma, por exemplo, de normas específicas para alguns setores de processamento de dados (para o setor de saúde ou de crédito ao consumo). Hoje, pode-se afirmar que um tal modelo de proteção de dados pessoais é representado pelos países europeus que transcreveram para seus ordenamentos as Diretivas europeias em matéria de proteção de dados, em especial a já mencionada Diretiva 95/46/CE e a Diretiva 2000/58/CE (conhecida como Diretiva sobre privacidade e as comunicações eletrônicas[387].

3. O CENÁRIO BRASILEIRO NA PROTEÇÃO DE DADOS PESSOAIS

---

[385] Ibid., p. 135-139.
[386] MAJONE, Giandomenico. **Do Estado Positivo ao Estado Regulador: Causas e Consequencias de Mudança do Modo de Governança**. Revista de Serviço Público, v. 50, n. 1, 1999.
[387] DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico Journal of Law [EJJL], v. 12, n. 2, 2011, p.101-102. Disponível em: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315>. Acesso em: 10 de Agosto de 2011, p.98.

Defende Jürgen Habermas que "O Estado moderno não nasce singular, mas como sistema de Estados", em que os arranjos econômicos e o próprio exercício da soberania, deixam de ser exercidos singularmente, e passam a operar reciprocamente entre as nações[388].

Na mesma direção, mas com especial atenção ao fenômeno tecnológico encetado na década de 70, resume bem Manuel Catells:

> Uma nova economia surgiu em escola global no último quartel do século XX. Chamo-a de informacional, global e em rede para identificar suas características fundamentais e diferenciadas e enfatizar sua interligação. É *informacional* porque a produtividade e a competitividade de unidades ou agentes nessa economia (sejam empresas, regiões ou nações) dependem basicamente de sua capacidade de gerar, processar e aplicar de forma eficiente a informação[389].

Nesta nova formação econômica, informacional, global e em rede, o controle eficiente do fluxo de dados, passou a ser imperativo, sob pena de escanteamento econômico, social e cultural (ou cibercultural) da nação não atenta a necessidade de domínio da nova técnica, que funda um ciberespaço construído mutuamente entre os países, e tem no seu controle eficiente, o novo marco civilizatório[390].

Reconheceu-se assim, em todo o mundo, a necessidade da instituição de organismos independentes, e, fundamentalmente técnicos, para coordenar esta sociedade em rede. Em estudo realizado em 2017, pelo *International Conference of Protection and Privacy*, analisou-se pelo menos 87 Autoridades Nacionais de proteção de dados, estando elas presentes em todos os países desenvolvidos do mundo, concentrando-se na Europa (64%) e na América do Norte (10%), e com apenas 4% delas na América do Sul, representadas pela Argentina e Uruguai.[391]

A ausência no Brasil no estudo chama atenção. A nona economia no mundo, e o quarto país em número de usuários de internet[392], em flagrante atraso, só em 2019 criou uma Autoridade Nacional de Proteção de Dados, e, ainda assim, com eficácia limitada a Maio de 2021, em razão da Lei 14.010/20, que adiou a aplicação da sanções previstas na LGPD.

---

[388] HABERMAS, Jürgen. **Para a Reconstrução do Materialismo Histórico**. Tradução de Carlos Nelson Coutinho. São Paulo: Editora Brasiliense, 1983, p.230.

[389] CASTELLS, Manuel, **A sociedade em Rede**. v.1, 8ª ed., Tradução de Roneide Venancio Majer, São Paulo: Editora Paz e terra, 2005, p.119.

[390] LÉVY, Pierre. **Cibercultura**, Tradução de Carlos Irineu Costa. Editora 34, 2010. p. 123-125. Disponível em: <https://mundonativodigital.files.wordpress.com/2016/03/cibercultura-pierre-levy.pdf>. Acesso em 05 de Agosto de 2020, p. 111-112.

[391] ICDPC CENSUS 2017. **Counting on Commissioners: High level results od the ICPPC Census 2017**. 6 de Setembro de 2017. Disponível em: <https://globalprivacyassembly.org/wp-content/uploads/2017/09/ICDPPC-Census-Report-1.pdf>. Acesso em 10 de Agosto de 2020.

[392] EXAME. **Brasil é o 4º pais em número de usuários de internet**. Tecnologia. 3 de Outubro de 2017. Disponível em: <https://exame.com/tecnologia/brasil-e-o-4o-pais-em-numero-de-usuarios-de-internet/#:~:text=usu%C3%A1rios%20de%20internet.-,Com%20120%20milh%C3%B5es%20de%20pessoas%20conectadas%2C%20o%20Brasil%20fica%20atr%C3%A1s,Reino%20Unido%20(59%20milh%C3%B5es)>. Acesso em 11 de Agosto de 2020.

A presença ativa de uma Autoridade Nacional independente não é condição imposta apenas pelo Conselho da Europa, mas também para a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), que desde 2013, ao revisar diretrizes sobre privacidade de 1980, tornou necessária a consolidação de uma Autoridade Nacional alheia a interferências políticas, nos países integrantes do grupo[393].

A OCDE nos últimos anos passou a recomendar aos países integrantes do grupo, e aos que desejam entrar, como é o caso do Brasil[394], a efetivação de um órgão capaz de não só aplicar a legislação interna de proteção de dados, mas também de regular o fluxo de dados pessoais em consonância com os padrões internacionais, estimulando uma Autoridade que tenha em sua condução, agentes capazes de decidir livremente, de maneira técnica, e integrada as medidas dos demais países membros[395].

Ainda que o Brasil tenha estreitado laços com a OCDE, o sonhado ingresso na elite econômica global ainda não se consolidou, e um dos fatores, como apontam relatórios da Organização, é inexistência de uma estrutura capaz de proteger a transmissão de dados a nível global.

O Uruguai e a Argentina são os únicos países na América Latina, satisfatoriamente preparados, segundo a OCDE, para lidar com os dados pessoais de maneira segura[396].

Quanto à Argentina, é bom registrar que assim como ocorreu aqui, a primeira legislação prevendo a proteção de dados (Lei 25.326/2000[397]), criava uma Autoridade integrante da administração pública indireta, o que foi vetado pelo executivo da época (Decreto 995/00), transformando-a em ente da administração publica direta vinculada ao governo.

O modelo criado em 2.000, com início de vigência em 2001, sofreu sérias críticas, diante da dúvida sobre sua real autonomia, de maneira que em 2017, com a entrada em vigor da Lei nº 27.275/2016[398], criou-se a *Agencia de Acesso a La Información Pública*¸ que deixou de

---

393 OECD. **OECD Work on privacy**. Setembro de 2013. Disponível em: <https://www.oecd.org/fr/sti/ieconomie/privacy.htm>. Acesso em 12 de Agosto de 2020.

394 ESTADÃO. **Por vaga na OCDE governo articula criar órgão de proteção de dados na internet**. 13 de Abril de 2018. Disponível em: <https://economia.estadao.com.br/noticias/geral,por-vaga-na-ocde-governo-articula-criar-orgao-para-protecao-de-dados-na-internet,70002266200>. Acesso em 13 de Agosto de 2020.

395 OECD. **OECD Work on privacy**. Setembro de 2013. Disponível em: <https://www.oecd.org/fr/sti/ieconomie/privacy.htm>. Acesso em 12 de Agosto de 2020.

396 EUROPEAN COMISSION. **Adequacy decisions. How the EU determines if a non-EU has an adequate level protection**. Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>. Acesso em 13 de Agosto de 2020.

397 ARGENTINA. **Lei 25.326/2000**. Disponível em: <https://www.oas.org/juridico/PDFs/arg_ley25326.pdf>. Acesso em 09 de gosto de 2020.

398 ARGENTINA. **Lei nº 27.275/2016**. Disponível em: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/265949/norma.htm>. Acesso em 09 de agosto de 2020.

integrar o governo e passou à administração pública indireta[399], fazendo com que fosse reconhecida pela OCDE com órgão capaz de controlar os dados pessoais de acordo com os padrões internacionais[400]. A experiência Argentina serve de alerta para o Brasil.

Assim como ocorreu na maior parte dos países, a legislação brasileira de proteção de dados pessoais deve seus moldes desenhados à partir da GPDR, que instituiu diretrizes e princípios gerais comuns, a serem adotados por países que buscam manter relações econômicas e diplomáticas com os países membros.

Com a entrada em vigor do Regime Geral sobre Proteção de Dados da União Europeia (GPDR), em 2018, unificou-se as normas atinentes a matéria na Europa, criando um regime geral, no escopo de proteger os dados dos cidadãos europeus, não mais apenas no continente, mas em todo o globo[401].

A transferência Internacional de dados ficou condicionada a chamada "Decisão de Adequação", prevista no art. 45 da GPDR:

> Pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado. Esta transferência não exige autorização específica.[402]

Dessarte, a permutação de informações com os países membros da União Europeia, e consequentemente, com as demais nações sujeitas aos padrões estabelecidos por ela, fica condicionada a um nível de proteção de dados equivalente ao da DPGR.

A relevância do dispositivo, e a necessidade de se adequar a ele, reafirmou-se em decisão super recente, prolatada ainda durante a redação deste projeto, em que o Tribunal de Justiça Europeu, anulou acordo de transferência de dados realizado em 2015 com os Estados

---

[399] SIMÃO, Bárbara; OMS, Juliana; TORRES, Livia. **Autoridade de Proteção de dados na América Latina: Um estudo dos modelos institucionais da Argentina, Colômbia e Uruguai**. IDEC: São Paulo, 2019. Disponível em: <https://idec.org.br/publicacao/autoridade-de-protecao-de-dados-na-america-latina>. Acesso em 10 de agosto de 2020.

[400] EUROPEAN COMISSION. **Adequacy decisions. How the EU determines if a non-EU has an adequate level protection**. Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>. Acesso em 13 de agosto de 2020.

[401] EUROPEAN COMISSION. **Adequacy decisions. How the EU determines if a non-EU has an adequate level protection**. Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>. Acesso em 13 de agosto de 2020.

[402] EUROPEAN COMISSION. **Adequacy decisions. How the EU determines if a non-EU has an adequate level protection**. Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>. Acesso em 13 de agosto de 2020.

Unidos, por entender que a plataforma utilizada (*Privacy Shield*)[403], não atendia aos níveis de proteção estabelecidos de maneira equivalente ao GPDR.

Dentre os critérios estabelecidos pelo regime europeu, para a concessão da "decisão de adequação", está:

> Art.45. b) A existência e o efetivo funcionamento de uma ou mais autoridades de controlo independentes no país terceiro ou às quais esteja sujeita uma organização internacional, responsáveis por assegurar e impor o cumprimento das regras de proteção de dados, e dotadas de poderes coercitivos adequados para assistir e aconselhar os titulares dos dados no exercício dos seus direitos, e cooperar com as autoridades de controlo dos Estados-Membros[404];

Resta, pois, incontroverso, a necessidade do Brasil de fixar uma Autoridade Nacional de Proteção de Dados independente, e com atuação técnica, em assentimento com diretrizes internacionais, ao abrigo de ter suas relações econômicas, e mesmo as diplomáticas, enfraquecidas.

4. O DESENHO INSTITUCIONAL DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS

O GPDR europeu serviu de inspiração a LGPD brasileira, de modo que no primeiro, ficou consignado de maneira incontroversa a atuação independe e autônoma das Autoridades de controle, obrigando os países signatários a desenvolverem uma estrutura capaz de garantir a isenção de seus membros. Já na LGPD, ainda não está claro se o modelo adotado atenderá efetivamente estas necessárias diretrizes.

Nesse sentido, sustenta Danilo Doneda sobre a importância deste organismo não estar vinculado diretamente a um dos poderes constitucionais, tão pouco submetido hierarquicamente, "sob pena de perder sua independência". Defende também que "o escopo da tutela da qual visa este órgão supõe uma neutralidade frente às próprias razões de Estado, que seria intangível sem esta independência"[405].

A Agência Nacional de Proteção de Dados ainda nem se estabeleceu, e já surgem sérias e razoáveis dúvidas quanto sua capacidade de se manter independente. Os principais questionamentos giram em torno da nova constituição da ANPD, que passou a ser ente da

---

[403] CNBC. **EU court voids data-sharing pact with the U.S. in Facebook privacy case**. 16 de julho de 2020. Disponível em: <https://www-cnbc-com.cdn.ampproject.org/c/s/www.cnbc.com/amp/2020/07/16/european-court-rules-on-facebook-vs-schrems-case.html>. Acesso em 11 de agosto de 2020.
[404] EUROPEAN COMISSION. **Adequacy decisions. How the EU determines if a non-EU has an adequate level protection**. Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>. Acesso em 13 de agosto de 2020.
[405] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p.387.

administração pública direta, vinculada ao Ministério da Justiça, e não mais uma autarquia especial. De modo que, conforme sustenta Roberto Pfeiffer:

> Um alento ocorreu com a edição da Medida Provisória 869, de 27 de dezembro de 2018, que a princípio seria merecedora de efusiva celebração, por ter criado a Autoridade Nacional de Proteção de Dados. Porém, o órgão nela estabelecido é institucionalmente mais frágil do que o previsto originariamente nos dispositivos vetados, não lhe tendo sido garantida a necessária autonomia, o que poderá enfraquecer a sua atuação e assim restringir a efetividade da tutela de dados pessoais no Brasil[406].

Antes mesmo da criação da ANPD, a discussão sobre sua natureza esteve muito presente, de modo que o §1º e 2º do Art.55-A da Lei 13.853/19, que altera a LGPD, possibilitou o Poder Executivo, em até dois anos, transformar a Autoridade em entidade da administração pública indireta.

A manutenção da ANPD como atualmente formulada, gera reflexos capazes de colocar em xeque sua independência funcional e sua real autonomia decisória (prevista no art.55-B da Lei 13.853/19). Como no caso de recurso administrativo hierárquico, assegurado pelo art.56 da Lei. 9784/99, que seria endereçado ao próprio Presidente da República, muito embora a LGPD verse também sobre o tratamento de dados realizado pelo poder público, o que não exclui o chefe do executivo.

Intimamente ligada com a controvérsia sobre a vinculação da ANPD ao Ministério da Justiça, está o questionamento sobre a independência funcional de seus Diretores, e se com este formato, em que na prática há subordinação hierárquica, a atuação será verdadeira independente, assim como ocorre na GPDR e defendido em todo o mundo.

A preocupação reside ainda na possibilidade do afastamento prévio dos Diretores pelo Presidente (Art.55-E, §2º), e do Ministro Chefe da Casa Civil instaurar processo administrativo (Art.55-E, §1º).

Por fim, há ampla crítica sobre a possibilidade de nomeação de funcionários como cargo "DAS-5"[407] a Diretores da ANPD. Primeiro pela baixa responsabilidade dos agentes, segundo por afastar talentos e quadros altamente técnicos da Diretoria, e terceiro, e mais importante, pela dificuldade de funcionários hierarquicamente inferiores, sancionar membros do alto escalão público e fazer cumprir a LGPD[408].

---

[406] PJEIFFER, Roberto. **ANPD em busca de sua autonomia: é preciso aperfeiçoar a MP 869/2018**. CONJUR, 01 de Maio de 2019. Disponível em: https://www.conjur.com.br/2019-mai-01/garantias-consumo-anpd-busca-autonomia-preciso-aperfeicoar-mp. Acesso em 14 de agosto de 2020.

[407] BRASIL, **Portaria nº 121 de 27 de março de 2029**. Disponível em: <https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/68938212/do1-2019-03-28-portaria-n-121-de-27-de-marco-de-2019-68938049<. Acesso em 15 de agosto de 2020.

[408] CAMARA DOS DEPUTADOS. **Especialistas defendem independência da Autoridade Nacional de Proteção de Dados**. 09 de abril de 2020. Disponível em: <https://www.in.gov.br/materia/-

A Autoridade Nacional de Proteção de Dados, como hoje disposta pelo Decreto 10.474/20, muito embora criada por lei, tem sua estrutura assemelhada a uma autoridade executiva. Caso modificada sua natureza jurídica, consoante possibilita art.55-A, §1º, da Lei 13.853/2019, tornar-se-ia uma autarquia em regime especial, assim como as Agências Reguladoras.

Dessarte, como ensina Bresser Pereira, responsável por orquestrar a Reformas do Estado dos anos 90: "As agências reguladoras devem ser mais autônomas do que as executivas porque não existem para realizar políticas do governo, mas para executar uma função mais permanente que é essa de substituir-se aos mercados competitivos"[409], o que melhor se adequa aos padrões internacionais de controle de dados.

Além dos problemas descritos, há questões que superam uma análise normativa material, impondo-se a reflexão sobre a construção histórica da burocracia brasileira, da legitimidade democrática dos entes da administração pública não eleitos, e do desenvolvimento de mecanismos de responsabilização a serem utilizados na ANPD.

O Brasil tem o patrimonialismo arraigado em sua estrutura política desde os tempos de colônia, quando as oligarquias formadas pelos senhores de terra já confundiam o público e privado, "domínio pessoal e o coletivo, entre a casa e o Estado[410]".

Com o decorrer da história, a elite oligárquica vai migrando para os quadros burocráticos brasileiros, transferindo a lógica patrimonialista para o funcionalismo público, mantendo a percepção de que a coisa pública poderia ser dirigida a interesses privados[411]. As oligárquicas se transformam em tecnocratas, e com o aumento do intervencionismo do Estado no século XX, consolida-se no Brasil "anéis burocráticos", que se utilizam da estrutura burocrática para defenderem os interesses de determinados grupos [412].

O funcionamento político nacional nunca foi capaz de afastar estas práticas de sua estrutura, que após a reabertura democrática em 1985, materializou-se através do "loteamento

/asset_publisher/Kujrw0TZC2Mb/content/id/68938212/do1-2019-03-28-portaria-n-121-de-27-de-marco-de-2019-68938049>. Acesso em 15 de agosto de 2020.

[409] PEREIRA, Luiz Carlos Bresser. **A Reforma do estado dos anos 90: lógica e mecanismos de controle**. Brasília: Ministério da Administração Federal e Reforma do Estado (MARE), 1997, p.47.

[410] RAMALHO, Pedro Ivo Sebba. **A gramática política das agências reguladoras: comparação entre o Brasil e EUA**. 2007, Tese (Doutorado em Ciências Sociais) - Programa de Pós-Graduação em Ciências Sociais da UNB, Universidade de Brasília, Brasília - DF, 2007, p.25.

[411] HOLANDA, Sérgio Buarque. **Raízes do Brasil**, 26 ed., São Paulo: Companhia das Letras, 1995. p.144-145.

[412] CARDOSO, Fernando Henrique. **Autoritarismo e democratização**. Rio de Janeiro, Paz e Terra, 1975, p.213-125.

dos cargos públicos da administração indireta e das delegacias dos ministérios nos Estados para os políticos dos partidos vitoriosos"[413].

Embora possa parecer contraditório, controverter sobre um modelo iniciado ainda no século XIX, em um trabalho que tem como objetivo a discussão de uma Autoridade Nacional ligada ao que há de mais novo em termos tecnológicos, a ponderação é pertinente e necessária, já que apesar de ter sua função voltada para um mercado do futuro, tem sua formação ligada a uma estrutura burocrática historicamente corrompida.

Este olhar para o passado, está agudamente alinhado com as reflexões mais contemporâneas sobre a atuação da Agencias de controle de dados em torno do globo, mormente quanto ao procedimento de eleição de seus dirigentes e seu exercício técnico e independente[414].

Neste cenário, surgem mais duas questões passíveis de discussão. A primeira é se o procedimento adotado pela LGPD na escolha dos membros integrantes da ANPD, com a modificação introduzida pela Lei 13.853/19, é suficiente para garantir um quadro técnico e autônomo. O segundo, é se uma Autoridade técnica e independe é o bastante para dar a legitimidade democrática a um ente público que não tem a sua frente sujeitos eleitos, e ainda assim possui poderes que transitam entre a atividade executiva, legislativa e jurisdicional.

CONSIDERAÇÕES FINAIS

A estruturação de um sistema de proteção de dados eficiente e legítimo, é fator imperativo para o Brasil se alinhar com as melhores práticas internacionais, viabilizando não só acordos comerciais volumosos, geração de empregos ligados a tecnologia, inserção na sociedade de rede e protagonismo na cibercultura em desenvolvimento, mas também, claro, a proteção do direito fundamental a privacidade dos usuários nacionais.

Passam assim as Autoridades Nacionais de Proteção de Dados, diante desta reorganização social, pautada nas interações virtuais, a tutelarem direitos e a interferirem na vida privada dos usuários, de modo que uma vez consubstanciada sua independência técnica, cria-se a necessidade de refletir sobre sua legitimidade de atuação.

Transmutando-se a ANPD para uma autarquia especial, integrante da administração pública indireta, conforme possibilita art.55-A, §1º da Lei 13.853/2019, há, em nosso sentir,

---

[413] BRASIL. Câmara da Reforma do Estado. **Plano diretor da reforma do aparelho do Estado**. Brasília: MARE, 1995, p. 20. Disponível em: <http://www.bresserpereira.org.br/documents/mare/planodiretor/planodiretor.pdf>. Acesso em 17 de Agosto de 2020.

[414] EUROPEU, CONSELHO. **Manual da Legislação Europeia sobre Proteção de Dados**, 2014, p.122-125.

grande ganho no que toca a independência técnica e a autonomia funcional de seus membros. Todavia, surgem desta positiva mudança novas questões a serem estudadas, como a legitimidade democrática de sua atuação, quais os instrumentos de responsabilização e controle são os mais adequados, e quais os limites da ANPD.

Isto posto, partindo da crença, que teremos uma ANPD independente e autônoma com o avançar do tempo, surge um novo desafio, alinhar a estas necessárias características uma terceira, a legitimidade, uma vez que, como já narrado, o Brasil vem de um processo político em que o patrimonialismo sempre se manteve presente, mantido por tecnocratas, e, hodiernamente, concretizado através de um clientelismo e do loteamento de cargos da administração pública indireta.

REFERÊNCIAS

ADORNO, Theodor. **Dialética do esclarecimento**, Editora Schwarcz-Companhia das Letras, 1947.

ARAGÃO, Alexandre dos Santos (coord.). **O Poder Normativo das Agências Reguladoras**. 2 ed., Rio de Janeiro: Forense, 2011.

BENNET. Colin J., **Regulatory Privacy, Data protection and Public Policy in Europe and the United States**, Cornell University Press: Ithaca and London, 1992.
BINENBOJM, Gustavo. **Agências Reguladoras Independentes e Democracia no Brasil**. Revista Eletrônica de Direito Administrativo Econômico, Salvador - BA, v.240, n.3, abr./jun. 2005.

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

BRASIL. Câmara da Reforma do Estado. **Plano diretor da reforma do aparelho do Estado**. Brasília: MARE, 1995.

CARDOSO, Fernando Henrique. **Autoritarismo e democratização**. Rio de Janeiro, Paz e Terra, 1975.

CARVALHO FILHO, José dos Santos. **Agências Reguladoras e o Poder Normativo**. In: ARAGÃO, Alexandre Santos (coord.), **O Poder Normativo das Agências Reguladoras**. 2 ed., Rio de Janeiro: Forense, 2011.

CASTELLS, Manuel, **A sociedade em Rede**. v.1, 8ª ed., Tradução de Roneide Venancio Majer, São Paulo: Editora Paz e terra, 2005.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico Journal of Law [EJJL], v. 12, n. 2, 2011

EUROPEU, CONSELHO. **Manual da Legislação Europeia sobre Proteção de Dados**, 2014.

FEENBER, Andrew. **Questioning Technology**. 3 ed.. Routeledge – Taylor & Francis Group: London and New York, 2001. p.207-209.

_____ **Transforming Technology, a critical theory revisited**. Oxford University Press: New York, 2002.

FERRAZ JÚNIOR, Tercio Sampaio. **Direito, Retórica e Comunicação: subsídios para uma pragmática do discurso jurídico.** 3.ed. São Paulo: Atlas, 2015.

_____ **O Poder Normativo das Agências Reguladoras à Luz do Princípio da Eficiência**. In: ARAGÃO, Alexandre Santos (coord.). **O Poder Normativo das Agências Reguladoras**. 2 ed., Rio de Janeiro: Forense, 2011.

FREIRE, Alonso. I**nterpretação constitucional comparativa: aproximação crítica e arcabouço metodológico**, Revista Publicum, v.2, n.1. p.45-73, 2016.

GENTOT, Michel. **Les Autorites Administratives Independantes**. Universite Claude Bernard Lyon I: Conseil d‘ etat, 1991.

GUERRA, Sérgio. **Agências Reguladoras – Da organização administrativa piramidal à governança em rede**. Belo Horizonte: Fórum, 2012.

GUTWIRTH, Serge; LEENES, Ronald; DE HERT, Paul; POULLET, Yves, **European Data Protection: In Good Health?**. Springer: London and New York, 2012.
HABERMAS, Jürgen. **Para a Reconstrução do Materialismo Histórico**. Tradução de Carlos Nelson Coutinho. São Paulo: Editora Brasiliense, 1983.

_____ **Técnica e Ciência como "ideologia**". Tradução de Artur Mourão. Edições 70: Lisboa, 1968.

HOLANDA, Sérgio Buarque. **Raízes do Brasil**, 26 ed., São Paulo: Companhia das Letras, 1995.

JUSTEN FILHO, Marçal. **Agências Reguladoras e Democracia: existe um déficit democrático na regulação independente?** In: ARAGÃO, Alexandre Santos (coord.), **O Poder Normativo das Agências Reguladoras**. 2 ed., Rio de Janeiro: Forense, 2011.

LÉVY, Pierre. **Cibercultura**, Tradução de Carlos Irineu Costa. Editora 34, 2010.

MAJONE, Giandomenico. **Do Estado Positivo ao Estado Regulador: Causas e Consequencias de Mudança do Modo de Governança**. Revista de Serviço Público, v. 50, n. 1, 1999.

MARCUSE, Herbert. **A ideologia da sociedade industrial: o homem unidimensional.** 4 ed. Tradução de Giasone Rebuá. Rio de Janeiro: Zahar Editores, 1973.

_____**Algumas implicações sociais da tecnologia moderna**. In: MARCUSE, Herbert; KELLNER, Douglas (ed.), **Tecnologia, Guerra e Fascismo**. Fundação Editora da Unesp: São Paulo, 1999.

MATTOS, Paulo Todescan Lessa. **O novo Estado regulador no Brasil: eficiência e legitimidade**. São Paulo: Editora Revista dos Tribunais, 2017.

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

NEDER, Ricardo T. (org.). **A teoria crítica de Andrew Feenberg. racionalização democrática**, **poder e tecnologia**. Escola de Altos Estudos da Capes: Brasília, 2013.

PEREIRA, Luiz Carlos Bresser. **A Reforma do estado dos anos 90: lógica e mecanismos de controle**. Brasília: Ministério da Administração Federal e Reforma do Estado (MARE), 1997.

RAMALHO, Pedro Ivo Sebba. **A gramática política das agências reguladoras: comparação entre o Brasil e EUA**. 2007, Tese (Doutorado em Ciências Sociais) - Programa de Pós-Graduação em Ciências Sociais da UNB, Universidade de Brasília, Brasília - DF, 2007.

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

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. **O direito à proteção de dados pessoais na sociedade da informação**. Revista Direito, Estado e Sociedade, n. 36, 2010.

SIMÃO, Bárbara; OMS, Juliana; TORRES, Livia. **Autoridade de Proteção de dados na América Latina: Um estudo dos modelos institucionais da Argentina, Colômbia e Uruguai**. IDEC: São Paulo, 2019.

WALD, Arnoldo; MORAES, Luiza Rangel de. **Agências Reguladoras**. Revista de Informação Legislativa, v. 36, n. 141, Brasília - DF, 1999.

WARREN, Samuel D.; BRANDEIS, Louis D. **The right to privacy**. Harvard law review, v. 4, n. 5, p. 193-220, 1980.

A (IM)POSSIBILIDADE DA EXTINÇÃO DAS OBRIGAÇÕES TRIBUTÁRIAS POR MEIO DAS CRIPTOMOEDAS

Roney Sandro Freire Corrêa
Plinio Lacerda Martins
Carlos Alberto Pereira de Aguiar

INTRODUÇÃO

O presente artigo tem como escopo analisar o mercado de criptomoedas, procurando compreender a temática a partir da ausência regulatória, objetivando responder à seguinte indagação: segundo as normativas do direito brasileiro, é possível pagar tributos utilizando criptomoedas?

A metodologia adotada é qualitativa, por meio de artigos científicos, pesquisa bibliográfica e documental, análise da regulamentação normativa no direito pátrio em cotejo com o direito comparado, adotando o método dedutivo-propositivo.

Inicialmente, cabe ressaltar que os fenômenos históricos da humanidade guardam uma ululante ligação com as finanças. Impérios foram construídos e destruídos, guerras travadas e políticas implementadas, frequentemente pautado em torno de uma lógica pecuniária.

O dinheiro é uma instituição social que tem demonstrado grande capacidade de evolução e adaptação ao caráter da sua época. É difícil de se imaginar uma sociedade que possa funcionar sem o dinheiro. No passado, isso já foi possível. Vivíamos na era do escambo, cujas relações eram lastreadas nas trocas de commodities e passamos também pela era dos metais, fato esse observado no Império Inca.[415] Foi a partir daí que a sociedade evoluiu para os metais preciosos como o ouro, surgindo mais tarde o papel-moeda, cujo valor era definido pela própria sociedade. Nesta fase, que durou até o século XIX, o dinheiro privado foi comum - nenhum governo sequer pensou em reivindicar um monopólio formal sobre a emissão e uso do dinheiro dentro de seu território político, o que só ocorreu com a consolidação formal dos poderes do Estado-nação[416].

A era do dinheiro em espécie, com características territoriais e com nuances determinadas por cada país, atingiu seu apogeu em meados do século XX com a invenção do controle de câmbio e capitais. Foi uma época em que o dinheiro passou a ser orientado por uma lógica de poder. Os símbolos

[415] FERGUSON, Niall. **A ascensão do dinheiro**: a história financeira do mundo. Tradução de Cordelia Magalhães. São Paulo: Planeta do Brasil, 2009. p. 23.

[416] COHEN, B. J. Electronic Money: New Day or False Dawn? **Review of International Political Economy.** p.197-225, v.8, n.2, 2001. p. 207.

de cada nação, fotos de figuras ilustres como reis e rainhas, passaram a ser estampados nas notas e moedas como forma de prestígio.

A partir das inovações tecnológicas, impulsionado pela economia digital, a tendência do consumo e das finanças mudou drasticamente, tendo o mercado de notas dado lugar ao dinheiro de plástico e, na sequência, à moeda virtual. Essa dinâmica iniciou-se em 1993, quando o matemático David Chanun[417] lançou o projeto *e-cash*, que muitos atribuem o seu fracasso por ter buscado ajuda de governos e bancos, que se viram ameaçados por uma iminente descentralização e, consequentemente, perda de poder. Surgia ali o embrião de um sistema de pagamentos eletrônicos, que anos mais tarde viria a revolucionar não só a sistemática dos meios de pagamento, mas postular um novo desafio quanto ao papel dos Estados ante a lógica do mundo digital.

Naquele momento, empresas como a Microsoft experimentaram incluir este mecanismo em seus *softwares*, não surtindo efeitos em razão de ameaças à segurança e privacidade, fatores considerados indispensáveis para o sucesso do projeto[418].

Em 1998, sob a ideologia libertária de Wei Daí, surgiu o *B-Money*, formulado sob a perspectiva de descentralizar o poder estatal do controle das operações financeiras ao desenvolver um sistema de protocolo não identificado e irrastreável, apto a troca de informações e estruturação de contratos[419].

Na sequência, surgiu o *Bit Gold*. Nick Szabo, além de lançar mão dos *smart contracts*, que foi o pilar do protocolo *blockchain*, projetou, anos mais tarde, o que seria a semente das criptomoedas[420].

Foi por meio de uma lista de discussão *cypherpunk*, que o programador com pseudônimo de Satoshi Nakamoto publicou, em 9 laudas, as diretrizes de algo que revolucionaria a economia digital, os Bitcoins[421].

---

[417] FERGUSON, Niall. **A ascensão do dinheiro:** a história financeira do mundo. Tradução de Cordelia Magalhães. São Paulo: Planeta do Brasil, 2009.

[418] TAPSCOTT, Alex; TAPSCOTT, Don. ***Blockchain Revolution***: como a tecnologia por trás do Bitcoin está mudando o dinheiro, os negócios e o mundo. São Paulo: Senai, 2016. p. 34.

[419] ROCHA, Luciano. ***Wei Dai***: como o seu B-Money inspirou a criação do Bitcoin, jun. 2018. Disponível em: <www.criptomoedasfacil.com/wei-daí-como-o-seu-b-money-inspirou-a-criacao-do-bitcoin> Acesso em: 18 jan. 2021.

[420] STANKOVIC, Stefan. **Who is Nick Szabo**, the mysterious blockchain titan, jul. 2018. Disponível em: <www.unblock.net/nick-szabo> Acesso em: 18 jan. 2021.

[421] MANGUEIRA, A. C. dos Santos. **Bitcoin**: uma análise da trajetória do dinheiro – Do escambo às criptomoedas : um estudo das legislações vanguardistas e suas influências sobre o projeto de lei n. 2.303/15. Recife: Unicape, 2018. 195 f. Dissertação (Mestrado em Direito) - Programa de Pós-graduação em Direito, Universidade Católica de Pernambuco, Recife, 2018.

Para alguns, o criador nunca foi revelado. Determinadas pessoas acreditam que Satoshi Nakamoto, na verdade, é formado por um grupo de empresas, sendo: Samsung, Toshiba, Nakamichi e Motorola, cujas inicias compõem o pseudônimo de seu inventor[422]. Há quem considere que o criador trata-se de Nick Szabo, pelas semelhanças e nuances apresentadas no projeto do *Bit Gold*.

Enfim, independentemente da autoria, o sistema foi formulado com diversas nuances, preenchendo lacunas suscitadas ante ao fracasso do *e-cash* e caracterizado pela indispensabilidade de intermediários financeiros, capaz de viabilizar segurança e proteção de cada transação, evitando que recursos fossem gastos em duplicidade[423].

Em continuidade, precisamente em janeiro de 2009, Nakamoto lançou livremente um *software* em um ambiente colaborativo com desenvolvedores, disponibilizando-o para quem quisesse fazer o download, a fim de construir um sistema de rede de Bitcoins. Destaca-se que esta colaboração ocorreu até 2011, quando, sem aviso prévio, novamente ele desapareceu. Antes de sumir, Nakamoto acumulou cerca de um milhão de sua criptomoeda[424].

O projeto obteve diversas críticas, desafiando países no processo de regulação, na tentativa de se valer do papel de centralizador e regulador das operações financeiras, sob forte ameaça de um ambiente de perda arrecadatória e de controle.

Não obstante, naquele momento, operações envolvendo criptomoedas já eram uma realidade e seus atores já vislumbravam uma redução de custo de operações sem a necessária intervenção estatal, lastreados em significativa segurança e notoriedade comercial, gerando inclusive um interesse da mídia, que se prestou a difundir a criação de outras moedas virtuais.

A tecnologia *blockchain* tornou-se uma indústria de grande impacto e de rápida ascensão, apontando como elemento imprescindível para diversos segmentos do futuro da humanidade, de modo que os fenômenos econômicos e sociais serão determinantes para influenciar conceitos jurídicos e determinar novas formas de se fazer negócios, desafiando os Estados quanto ao seu poder de tributar.

---

[422] LIVECOINS. **História dos Bitcoins**. Disponível em: <https://livecoins.com.br/historia-do-bitcoin/> Acesso em: 18 jan. 2021.

[423] NAKAMOTO, Satoshi. **Bitcoin:** *A Peer-to-Peer Electronic Cash System*. Disponível em: <https://bitcoin.org/bitcoin.pdf> Acesso em: 18 jan. 2021.

[424] LIVECOINS. **História dos Bitcoins**. Disponível em: <https://livecoins.com.br/historia-do-bitcoin/> Acesso em: 18 jan. 2021.

Em solo brasileiro, os desafios são ainda maiores, tendo em vista que seu arranjo tributário é datado da década de 1960, uma época em que as operações mercantis eram exclusivamente para bens corpóreos e formuladas para atender modelos tradicionais de realização de negócios.

De lá para cá, o mundo se virtualizou e a intangibilidade tornou progressivamente a presença física em determinada localidade desnecessária. Com a instituição das criptomoedas, a intermediação também acompanhou essa tendência.

Pensando nisso, em 2020, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), manifestou a sua preocupação quanto às consequências tributárias desse novo mercado, por representar um potencial risco à transparência fiscal e financeira, definindo diversas orientações e recomendações[425].

Klaus Schwab mencionou que em 2030, versões de "*blockchains* poderão revolucionar tudo, desde transações financeiras até a forma em que votamos". A realidade está posta, atualmente são negociados 4.085 tipos diferentes de criptomoedas com mais de 700 bilhões [426] de dólares transacionados[427].

1. AS CRIPTOMOEDAS: CARACTERÍSTICAS, DESTERRITORIALIZAÇÃO E DESINTERMEDIAÇÃO

As criptomoedas referem-se a um termo geral para descrever ativos digitais criptografados com tecnologia *blockchain*. O uso deste termo é enganoso, pois implica que todos esses ativos digitais atendem à definição de moeda ou dinheiro, ou seja, que representam uma unidade de conta, uma reserva de valor e um meio de troca. Esse não é sempre o caso.

As criptomoedas dividem-se em duas categorias: as moedas de *criptocurrency* alternativas e os *tokens*. Embora os termos "moedas" e "*tokens*" sejam frequentemente usados de forma intercambiável, existem diferenças significativas entre essas duas categorias.

---

[425] ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. **Taxing Virtual Currencies**: An Overview Of Tax Treatments And Emerging Tax Policy Issues. Paris: OECD. Disponível em: <www.oecd.org/tax/tax-policy/taxing-virtual-currencies-an-overview-of-tax-treatments-and-emerging-tax-policy issues.htm> Acesso em: 18 jan. 2021.

[426] TAPSCOTT, Alex; TAPSCOTT, Don. **Blockchain revolution**: como a tecnologia por trás do Bitcoin está mudando o dinheiro, os negócios e o mundo. São Paulo: Senai, 2016. p. 143.

[427] COINMARKETCAP. Today's Cryptocurrency Prices by Market Cap. Disponível em: <https://coinmarketcap.com> Acesso em: 18 jan. 2021.

Moedas, por exemplo, Ethereum, Bitcoins, Altcoins etc., são tipos de criptomoedas que operam independentemente de qualquer outra plataforma. Em outras palavras, uma moeda tem sua própria plataforma movida a *blockchain*. O objetivo de uma moeda é agir como dinheiro. Em contraste, um *token* é um valor de unidade que existe em um *blockchain* existente[428].

Embora comumente associado ao Bitcoin, o *blockchain* pode ser usado para propósitos diferentes que vão muito além das moedas digitais. Podemos pensar no *blockchain* como um sistema operacional e o Bitcoin apenas como uma das muitas possibilidades de execução desse sistema.

Em termos simples, *blockchain* é um livro-razão aberto e distribuído que pode registrar transações entre duas partes de forma eficiente, verificável e permanente. Nesse escopo, cinco pilares fundamentais sustentam a tecnologia de *blockchain*, assim determinados: banco de dados distribuído, controle descentralizado, transmissão ponto a ponto, o que se denomina *peer to peer exchange*, irreversibilidade dos registros e o pseudo-anonimato.

Existem *blockchains* públicos e privados. Em um *blockchain* público, todos podem visualizar seu conteúdo, conduzir transações e contribuir para a segurança e integridade do *blockchain*. As vantagens dessa abordagem são um alto nível de segurança, baixos custos e prevenção de erros individuais em potencial. As principais desvantagens são a escalabilidade limitada e a transparência invariável de todas as transações, o que está em conflito com questões de privacidade.

Em *blockchains* privados ou centralizados, existe alguma forma de administração central ou pelo menos um número limitado de participantes. Assim é o Bitcoin, no qual é transferido de um computador para outro, por meio de um sistema de *hashes* criptográficos e mantido em segurança por meio de criptografia de chave pública-privada. Cada transação de pagamento é transmitida para a rede e incluída na cadeia de bloqueio, de forma que os Bitcoins usados não podem ser gastos duas vezes. Novos Bitcoins são gerados de maneira distribuída e a uma taxa previsível.

> Em poucas palavras, o Bitcoin é uma forma de dinheiro, assim como o real, o dólar ou o euro, com a diferença de ser puramente digital e não ser emitido por nenhum governo. O seu valor é determinado livremente pelos indivíduos no mercado. Para transações online, é a forma ideal de pagamento, pois é rápido e seguro[429].

[428] TAPSCOTT, Alex; TAPSCOTT, Don. **Blockchain revolution**: como a tecnologia por trás do Bitcoin está mudando o dinheiro, os negócios e o mundo. São Paulo: Senai, 2016.

[429] ULRICH, Fernando. **Bitcoin:** a moeda na era digital. São Paulo: Instituto Ludwig Von Mises Brasil, 2014. p.16.

Um dos principais benefícios do uso do Bitcoin, além do seu amplo crescimento em aceitação, é a falta de taxas de transação associadas à transferência de fundos, visto que as transações ocorrem em uma rede ponto-a-ponto. No Brasil, em julho de 2014, apenas 79 estabelecimentos comerciais declaravam aceitar Bitcoins, já em 2016, o número passou para 7.545 e, em 2019, atingiu a marca de 15.848[430], o que demonstra não somente o incremento deste mercado, mas o seu nível de aceitação.

Por outro lado, o uso de moeda descentralizada também acarreta riscos, sobretudo pela sua dinâmica de alta oscilação e desregulamentação, fatores de ameaça aos seus usuários. Fato este que pode ser ilustrado por meio da representação gráfica abaixo, onde é possível notar que o preço de cada Bitcoin, no período de 10 anos, variou de 0,06 a 11.856,50 dólares:

Fonte: *Buy Bitcoin World Wide*[431]

2. AS CRIPTOMOEDAS COMO INSTRUMENTO DE EXTINÇÃO DAS OBRIGAÇÕES TRIBUTÁRIAS ANTE AS EXPERIÊNCIAS COMPARADAS

O mercado de criptomoedas apresenta uma fluidez de termos adotados por diferentes países ao descrever diferentes produtos que se enquadram em seu âmbito. Alguns compreendem a

[430] GUARACI, Neto. Número de lojas que aceitam bitcoin cresce 13% em 2019. CoinTimes, 2020. Disponível em: <https://cointimes.com.br/numero-de-lojas-que-aceitam-bitcoin-cresce-13-em-2019/> Acesso em: 18 jan. 2021.

[431] BUY BITCOIN WORLD WIDE. Gráfico do histórico de preço do Bitcoin, ago. 2010 a ago.2020. Disponível em: <https://www.buybitcoinworldwide.com/pt-br/preco/> Acesso em: 18 jan. 2021.

criptomoeda como moeda digital, como no caso da Argentina e Austrália, outros como mercadoria virtual, como Canadá e China. Em outra jurisdição, como no caso da Suíça, considera-se a criptomoeda como token de pagamento, na Itália e Líbano como moeda cibernética, e Honduras e México como ativo virtual[432].

Ante a ausência de uniformidade, a cada ano o número de jurisdições que aceitam a criptomoeda como meio de pagamento tem aumentado progressivamente. Em alguns países é aceita até mesmo por seus órgãos governamentais. Em outros, como a Ilha de Man e o México, permitem o uso como meio de pagamento em paralelo à moeda pátria[433].

Essas experiências têm compelido diversos países a adotarem a tecnologia a seu favor, sobretudo quanto ao incremento de negócios e facilitação da extinção de suas obrigações tributárias por meio de pagamento.

Pioneiramente, as cidades suíças de Zug e Ticino, se tornaram as primeiras a aceitarem que seus contribuintes pudessem efetuar pagamentos de tributos por meio de criptomoedas[434].

Na sequência, os estados norte-americanos de Ohio, New Hampshire e Utah[435], também iniciaram a aceitação desta modalidade de pagamento para a quitação de suas obrigações tributárias[436].

A Austrália, ainda que não aceite as criptomoedas como forma de pagamento para o exercício das obrigações tributárias, deu um passo adotando uma posição de atribuir o idêntico tratamento de sua moeda.

---

[432] The Law Library of Congress, Global Legal Research Center. **Regulation of Cryptocurrency Around the World**. Disponível em: <https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf> Acesso em: 18 jan. 2021.

[433] Ibid.

[434] MARQUES, Diego. Mundo: Estônia, Malta e Suíça estão entre os países líderes em blockchain. **Guia do Bitcoin**. Disponível em: <https://guiadobitcoin.com.br/noticias/estonia-malta-suica-paises-lideres-blockchain/> Acesso em: 18 jan. 2021.

[435] HOON, Iven de. Can I pay taxes with Bitcoin? **No More Tax.** Disponível em: <https://nomoretax.eu/can-i-pay-my-taxes-with-bitcoin/#:~:text=At%20present%2C%20the%20U.S.%20tax,directly%20for%20paying%20tax%20obligations.&text=Thus%2C%20any%20profits%20received%20through,deducted%20from%20the%20tax%20bill> Acesso em: 18 jan. 2021.

[436] MARQUES, Diego. Mundo: Estônia, Malta e Suíça estão entre os países líderes em blockchain. **Guia do Bitcoin**. Disponível em: <https://guiadobitcoin.com.br/noticias/estonia-malta-suica-paises-lideres-blockchain/> Acesso em: 27 jan. 2021.

No Canadá, as leis e regras tributárias também se aplicam às transações envolvendo a moeda digital, estando sujeitas ao imposto de renda. Em pequenas cidades do país, como Innisfil, no estado de Ontário, já se autoriza o pagamento de parte ou totalidade dos tributos sobre a propriedade por meio de criptomoedas[437].

No caso da Áustria, o governo publicou um aviso sobre o tratamento fiscal da moeda virtual. Na opinião do Ministro de Finanças daquele país, a moeda virtual deve ser classificada como um ativo intangível não depreciável, não constituindo um instrumento financeiro. Neste caso, se usada para fins comerciais, a moeda virtual deve ser geralmente tratada como outros ativos comerciais e sujeita às regras gerais do imposto de renda.[438]

3. O MERCADO DE CRIPTOMOEDAS NO BRASIL E A PERSPECTIVA LEGISLATIVA

No caso brasileiro, a questão é bastante peculiar, pois carece de um sistema regulatório que possa traduzir normativamente a moeda virtual como meio de pagamento.

O primeiro diploma a tratar sobre a matéria foi a Lei 12.865/2013, que abordou o tema no seu art. 6.º[439], considerando que instituições de pagamento podem ser conceituadas como aquelas pessoas físicas ou jurídicas que convertam moedas físicas ou estruturais em moedas eletrônicas, credenciando a sua aceitação ou gerando o uso de moeda eletrônica, estando inseridas no Sistema de Pagamentos Brasileiros e sujeitos a regulamentação do Banco Central e do Conselho Monetário Nacional.

Em 19 de fevereiro de 2014, o Banco Central do Brasil (BACEN), divulgou o primeiro comunicado atinente ao sistema Bitcoin.[440]. Naquela oportunidade, fez-se a distinção entre moedas virtuais e eletrônicas, mencionando que moedas virtuais nas denominadas carteiras eletrônicas

---

[437] INNISFIL. Paying Property Taxes With Bitcoin. Disponível em: <https://innisfil.ca/pay-with-bitcoin/> Acesso em: 18 jan. 2021.

[438] Disponível em: https://www.bmf.gv.at/steuern/kryptowaehrung_Besteuerung.html. Acesso em 18 de jan. de 2021.

[439] BRASIL. Lei Nº 12.865, de 9 de Outubro de 2013. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12865.htm> Acesso em: 28 jan. 2021.

[440] BRASIL. Comunicado nº. 25.306/2014. **Banco Central do Brasil**. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/buscanormas?dataInicioBusca=20%2F01%2F2010&dataFimBusca=23%2F01%2F2021&tipoDocumento=Comunicado> Acesso em: 18 jan. 2021.

apresentam riscos de que o detentor desses ativos sofra perdas patrimoniais decorrentes de ataques de criminosos que atuam no espaço da rede mundial de computadores.

Em 2017[441], o BACEN reiterou a sua preocupação, alertando que, uma vez que as moedas virtuais não são emitidas nem garantidas por qualquer autoridade monetária, os investidores devem arcar com todos os seus riscos relacionados à fraude, roubo e desvalorização.

Naquele mesmo ano, a Comissão de Valores Mobiliários (CVM) emitiu um aviso esclarecendo que moedas virtuais não são títulos e, portanto, não podem ser adquiridas por fundos de investimento locais, já que a Lei 6.385/1976[442] não inclui os Bitcoins, ou outras criptomoedas, no rol dos demais valores mobiliários[443].

Tal entendimento foi corroborado em decisão do Superior Tribunal de Justiça, quando analisou o conflito de competência nº 161.123[444] e o HC 530.563-RS[445], sustentando a inexistência da regulação das criptomoedas no ordenamento pátrio, não sendo nem moeda, conforme sustenta o BACEN, nem valor mobiliário, como sustenta a Comissão de Valores Mobiliários.[446]

---

[441] BRASIL. **BANCO CENTRAL DO BRASIL**. Comunicado nº 31.379. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/buscanormas?dataInicioBusca=20%2F01%2F2010&dataFimBusca=23%2F01%2F2021&tipoDocumento=Comunicado> Acesso em: 18 jan. 2021.

[442] BRASIL. Lei n 6.385, de 7 de Dezembro DE 1976. Dispõe sobre o mercado de valores mobiliários e cria a Comissão de Valores Mobiliários. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l6385.htm> Acesso em: 28 jan. 2021.

[443] BRASIL. **Comissão de Valores Mobiliários.** Disponível em: <http://www.cvm.gov.br/export/sites/cvm/legislacao/oficios-circulares/sin/anexos/oc-sin-0118.pdf> Acesso em: 18 jan. 2021.

[444] STJ - CC: 161123 SP 2018/0248430 -4, Relator: Ministro SEBASTIÃO REIS JÚNIOR, Data de Julgamento: 28/03/2018, S3 - TERCEIRA SEÇÃO, Data de Publicação: DJe 05/12/2018. **JusBrasil**, 2018. Disponível em: <https://stj.jusbrasil.com.br/jurisprudencia/661801952/conflito-de-competencia-cc-161123-sp-2018-0248430-4/inteiro-teor-661801962> Acesso em: 28 jan. 2021

[445] STJ - HC: 530563 RS 2019/0259698-8, Relator: Ministro SEBASTIÃO REIS JÚNIOR, Data de Publicação: DJ 05/09/2019. **JusBrasil**, 2019. Disponível em: <https://stj.jusbrasil.com.br/jurisprudencia/877693098/habeas-corpus-hc-530563-rs-2019-0259698-8> Acesso em: 28 jan. 2021.

[446] BRASIL. Informativo de Jurisprudência. **Superior Tribunal de Justiça**. Disponível em: <https://www.stj.jus.br/publicacaoinstitucional/index.php/informjuris/article/viewFile/3859/4085> Acesso em: 18 jan. 2021. p. 138.

Ante a confusão terminológica, não sendo nem moeda, nem valor mobiliário, a Secretaria da Receita Federal, a seu turno, foi uma das primeiras instituições governamentais a equiparar as criptomoedas ao "Ativo Financeiro"[447].

Na sequência, a Secretaria da Receita Federal publicou a instrução normativa nº 1888, aduzindo criptoativos como:

> a representação digital de valor denominado em sua própria unidade de conta, cujo preço pode ser expresso em moeda soberana local ou estrangeira, transacionado eletronicamente com a utilização de criptografia e de tecnologias de registros distribuídos, que pode ser utilizado como forma de investimento, instrumento de transferência de valores ou acesso a serviços, e que não constitui moeda de curso legal.[448]

Tal definição não foi o bastante para o processo de sua regulamentação, desconsiderando a evolução das formas de pagamentos que vêm sendo utilizadas em diversos países.

Não obstante, surgiram projetos de lei, tanto na Câmara dos Deputados, quanto no Senado Federal, que pretendem definir "arranjos de pagamento" e regulamentar o regime jurídico das criptomoedas.

O certo, é que esta letargia, ao determinar uma medida regulatória, ante ao amplo interesse contraditório em avançar no processo de normatização e aceitação desta nova tipologia revela, não somente um descompasso com relação ao outros países, mas orienta a perda de competitividade e o aprofundamento da insegurança jurídica.

4. A EXTINÇÃO DA OBRIGAÇÃO TRIBUTÁRIA: A (IM)POSSIBILIDADE DO PAGAMENTO DE TRIBUTOS POR MEIO DE CRIPTOMOEDAS

[447]BRASIL. Perguntas e Respostas: Imposto sobre a Renda da Pessoa Física, IRPF. **Secretaria da Receita Federal**. 2020. Disponível em: <https://receita.economia.gov.br/interface/cidadao/irpf/2020/perguntao/p-r-irpf-2020-v-1-3-2020-10-27.pdf> Acesso em: 18 jan. 2021. p. 186.

[448] BRASIL. Instrução Normativa RFB nº 1888, de 03 de Maio de 2019. Institui e disciplina a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos à Secretaria Especial da Receita Federal do Brasil (RFB). Receita Federal. Disponível em: <http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=100592> Acesso em: 28 jan. 2021

Introduzida no Código Tributário Nacional como uma das modalidades de extinção do crédito tributário, cujo pagamento é a forma mais emblemática e imediata para a extinção da obrigação tributária.

Conforme preceitua o art. 3º do Código Tributário Nacional[449], a obrigação tributária é sempre pecuniária, ou seja, só pode ser solvida em dinheiro ou em valor que se possa exprimir.

Segundo o art. 162 do Código Tributário Nacional[450], o pagamento só pode ser extinto em moeda corrente, cheque ou vale postal e nos casos previstos em lei, em estampilha, papel selado ou por processo mecânico.

A Constituição ofertou um conceito de "moeda" ao qual não pode ser transferido diretamente às criptomoedas. Segundo os arts. 21, VII, 48, XIV e 164[451], compete à União, por meio do Banco Central, conforme regras ditadas pelo Congresso Nacional, emitir moeda e regular sua oferta.

Ante o exposto, as criptomoedas não são legalmente consideradas meios de pagamentos aptos e suficientes para promover a extinção do crédito tributário. Entretanto, é interessante observar duas situações em que a Receita Federal se presta a reconhecer a tributação das criptomoedas e o reconhecimento da sua atividade de mineração, equiparando-a aos rendimentos laborais.

Na primeira, reconhece que há a tributação dos ganhos obtidos com a alienação de criptomoedas, a título de ganho de capital. Na segunda, a Receita Federal entende e equipara a atividade de mineração ao rendimento decorrente do trabalho. Em consonância com o art. 457 da Lei nº 13.467/17[452], o produto do trabalho tem como necessária a contraprestação remuneratória.

Em ambos os casos, as críticas caminham quanto ao reconhecimento da tributação das criptomoedas e da equiparação da atividade mineradora como rendimento decorrente de trabalho, ao se constatar que a determinação da obrigação tributária é de natureza pecuniária, só podendo ser solvida em dinheiro ou em valor que se possa exprimir, ou seja, neste caso, como ativo financeiro.

---

[449] BRASIL. Código Tributário Nacional. Lei no 5.172, de 25 de Outubro de 1966. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L5172.htm> Acesso em: 28 jan. 2021.

[450] BRASIL. Código Tributário Nacional. Lei no 5.172, de 25 de Outubro de 1966. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L5172.htm> Acesso em: 28 jan. 2021.

[451] BRASIL. **Constituição 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> Acesso em: 18 jan. 2021.

[452] BRASIL. Lei nº 13.467, de 13 de Julho de 2017. Altera a Consolidação das Leis do Trabalho (CLT), aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943, e as Leis n º 6.019, de 3 de janeiro de 1974. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13467.htm> Acesso em: 28/01/21.

Esse entendimento é de fundamental importância para o incremento arrecadatório por parte do Estado, ao facilitar a extinção das obrigações tributárias mediante pagamento por criptomoedas, bem como viabilizar a identificação e a coibição de práticas delituosas.

CONSIDERAÇÕES FINAIS

Este artigo procurou analisar os desafios e as principais dificuldades enfrentadas pela regulação das moedas virtuais pelo poder público brasileiro, procurando comparar experiências deflagradas em diversos países, objetivando analisar a temática ante a perspectiva de ser uma modalidade apta para o exercício de extinção das obrigações tributárias.

Em um cenário vigorante, de profundas dificuldades fiscais, acentuado pelo quadro da pandemia mundial da COVID-19, qualquer recurso ou meio de pagamento lícito deveria ser validado, tendo a regulação um elemento estratégico a fim de viabilizar o crescimento do próprio mercado de criptomoedas.

O país não pode se valer do negacionismo e isolacionismo em relação às medidas adotadas pelas demais nações, especialmente por estarmos inseridos em um ambiente altamente globalizado, cujo fluxo de investimentos e de transações não sustentam sua inação.

Se não bastasse a peculiaridade do modelo tributário datado do século passado, antes mesmo dos avanços tecnológicos, os atos regulatórios e normativos referentes às criptomoedas se revelam insuficientes, inadequados e inseguros ante uma perspectiva jurídica.

Como prova a análise das experiências deflagradas em diversas jurisdições, os países avançam no sentido de viabilizar as criptomoedas como instrumento de facilitação de negócios, demonstrando sua viabilidade e reconhecimento como se moeda fosse.

Os países que tentarem postergar o efeito desta realidade, além de se tornarem meros expectadores, serão absorvidos pelos efeitos decorrentes da quarta revolução industrial em curso, a tecnológica[453].

REFERÊNCIAS BIBLIOGRÁFICAS

[453] SCHWAB, Klaus. **A quarta revolução industrial**. Tradução de Daniel Moreira Miranda. São Paulo: Edipro, 2016.

COHEN, B. J. Electronic Money: New Day or False Dawn? Review of International Political Economy. p.197-225, v.8, n.2, 2001..

BRASIL. Comunicado nº. 25.306/2014. **Banco Central do Brasil**. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/buscanormas?dataInicioBusca=20%2F01%2F2010&dataFimBusca=23%2F01%2F2021&tipoDocumento=Comunicado> Acesso em: 18 jan. 2021.

BRASIL. **BANCO CENTRAL DO BRASIL**. Comunicado nº 31.379. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/buscanormas?dataInicioBusca=20%2F01%2F2010&dataFimBusca=23%2F01%2F2021&tipoDocumento=Comunicado> Acesso em: 18 jan. 2021.

BRASIL. **Comissão de Valores Mobiliários.** Disponível em: <http://www.cvm.gov.br/export/sites/cvm/legislacao/oficios-circulares/sin/anexos/oc-sin-0118.pdf> Acesso em: 18 jan. 2021.

BRASIL. **Constituição 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> Acesso em: 18 jan. 2021.

BRASIL. Perguntas e Respostas: Imposto sobre a Renda da Pessoa Física, IRPF. **Secretaria da Receita Federal**. 2020. Disponível em: <https://receita.economia.gov.br/interface/cidadao/irpf/2020/perguntao/p-r-irpf-2020-v-1-3-2020-10-27.pdf> Acesso em: 18 jan. 2021.

BRASIL. Informativo de Jurisprudência. **Superior Tribunal de Justiça**. Disponível em: <https://www.stj.jus.br/publicacaoinstitucional/index.php/informjuris/article/viewFile/3859/4085> Acesso em: 18 jan. 2021.

BUY BITCOIN WORLD WIDE. **Gráfico do histórico de preço do Bitc**oin, ago. 2010 a ago.2020. Disponível em: <https://www.buybitcoinworldwide.com/pt-br/preco/> Acesso em: 18 jan. 2021.

FERGUSON, Niall. **A ascensão do dinheiro**: a história financeira do mundo. Tradução de Cordelia Magalhães. São Paulo: Planeta do Brasil, 2009

LIVECOINS. **História dos Bitcoins**. Disponível em: <https://livecoins.com.br/historia-do-bitcoin/> Acesso em: 18 jan. 2021.

MANGUEIRA, A. C. dos Santos. **Bitcoin**: uma análise da trajetória do dinheiro – Do escambo às criptomoedas : um estudo das legislações vanguardistas e suas influências sobre o projeto de lei n. 2.303/15. Recife: Unicape, 2018. 195 f. Dissertação (Mestrado em Direito) - Programa de Pós-graduação em Direito, Universidade Católica de Pernambuco, Recife, 2018.

NAKAMOTO, Satoshi. **Bitcoin:** A Peer-to-Peer Electronic Cash System. Disponível em: <https://bitcoin.org/bitcoin.pdf> Acesso em: 18 jan. 2021.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. **Taxing Virtual Currencies**: An Overview Of Tax Treatments And Emerging Tax Policy Issues. Paris: OECD. Disponível em: <www.oecd.org/tax/tax-policy/taxing-virtual-currencies-an-overview-of-tax-treatments-and-emerging-tax-policy issues.htm> Acesso em: 18 jan. 2021.

SCHWAB, Klaus. **A quarta revolução industrial**. Tradução de Daniel Moreira Miranda. São Paulo: Edipro, 2016.

TAPSCOTT, Alex; TAPSCOTT, Don. ***Blockchain Revolution***: como a tecnologia por trás do Bitcoin está mudando o dinheiro, os negócios e o mundo. São Paulo: Senai, 2016.

The Law Library of Congress, Global Legal Research Center. **Regulation of Cryptocurrency Around the World**. Disponível em: <https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf> Acesso em: 18 jan. 2021.

ULRICH, Fernando. **Bitcoin:** a moeda na era digital. São Paulo: Instituto Ludwig Von Mises Brasil, 2014.