REVISTA ELETRÔNICA DA PGE-RJ
ISSN 2595-0630
(DOI): 10.46818/pge.v5i2.268

PROTEÇÃO DE DADOS: VPNS E O ORDENAMENTO JURÍDICO BRASILEIRO.

DATA PROTECTION: VPNS AND BRAZILIAN LAW.

Samuel Medeiros Andreatta[1]

RESUMO: Trata-se de exploração crítica das nuances que comportam os serviços de empresas de VPN (Very Private Network). Percebeu-se, através de levantamento bibliográfico, o desenvolvimento de um panorama global de monitoramento e vigilância, que é entendido sob o conceito de sociedade de exposição. Neste panorama as VPNS se apresentam como um vetor de materialização da privacidade. Tais empresas criam um mercado centrado na mercantilização da sensação de segurança e privacidade na rede. A atuação específica dessas empresas carece de esclarecimentos técnicos aos titulares dos dados, o que pode fragilizar a autodeterminação informativa e a efetiva possibilidade de requisição de dados. Ademais, verificou-se que a legislação brasileira comporta alguns limites específicos na Lei Geral de Proteção de Dados e Marco Civil da Internet. Notadamente, no que diz respeito à guarda específica de registros no tratamento de dados por provedor de conexão, há algumas incongruências. Notou-se também uma abertura para a relativização do dever de exibição de uma clara finalidade no tratamento de dados no tocante à amplitude do conceito de segredo industrial e comercial. Por fim, conclui-se que a legislação específica acerca das empresas de VPN ainda está por ser elaborada uma vez que a legislação atual possui lacunas sobre o tema.

PALAVRAS-CHAVE: VPN - Privacidade – Vigilância - Lei geral de Proteção de dados

ABSTRACT: A critical exploration of the nuances that concern the services provided by VPN (Very Private Network) companies. It was noted, through bibliographical research, that there's been a development in the global scenario of surveillance, and it relates to a will to expose oneself. In this scenario, VPN companies can be perceived as boundary objects and present themselves as a vector that substantiates claims of privacy. They create a market centered in the commodification of a sense of security and privacy on the web. The way these companies operate shows a lack of availability of technical information concerning user data and can put the right to your own data and the effective possibility of the state gathering information in a precarious position. There is also an overconfidence in the algorithms that dictate the functioning of technology. Furthermore, it has been noted that the Brazilian law establishes a few specific limitations in the General Law of data protection and in the Civil Law of Internet. Notably, concerning the duty of the service provider to keep connection logs, a few inconsistencies have been perceived. Moreover, an opening for the relativization of the duty to show connection logs by the service provider has been perceived concerning the large spectrum of activities that can be framed as industrial or commercial secrets. The research concludes that Brazilian law lacks specific regulations that is yet to be sedimented by jurisprudence and by the National Authority of Data Protection so that these companies can act under a robust set of laws.

[1] Bacharel em Direito pela Universidade Federal do Rio de Janeiro(FND-UFRJ), Advogado Criminalista OAB/ RJ 229.526, mestrando bolsista CAPES PROSUC Modalidade I de Ciências Criminais na PUC- RS.

KEYWORDS: VPN – Privacy – Surveillance- General Law of Data Protection

SUMÁRIO: Introdução. 1. Aspectos críticos da VPN. 2. Marco Civil da Internet e VPN. 2.1. Lei Geral de Proteção de Dados e VPN. 3. Conclusão. Referências.

SUMMARY: Introduction. 1. Critical Aspects of VPN. 2. Marco Civil da Internet and VPN. 2.1. Data Protection Law and VPN. 3. Conclusion. References.

Introdução

Esse modelo já possui a formatação correta da página (Papel A4 com margens esquerda e superior em 3cm; margens direita e inferior em 2,0 cm) que não deve ser alterada. A formatação do parágrafo deve ser feita com recuo especial na primeira linha de 2,0 cm e o espaçamento entre linhas deve constar como 1,5 linhas, mantendo antes e depois em 0 pt. O corpo do texto deve ser formatado para Times New Roman em tamanho 12 como alinhamento justificado. Ressalto que este modelo foi elaborado dentro das regras estabelecidas, devendo ser mantido os espaços dados entre os tópicos. As páginas não devem ser numeradas.

O norte epistemológico deste trabalho incorpora a definição do cenário tecnológico através do desígnio *"sociedades de exposição*[2]*".* A exposição é um conceito que traduz a justaposição de forças panópticas[3], forças que propagam vetores da *sociedade de controle*[4], e práticas voluntárias que demarcam os processos de coleta de informação ligadas a um desejo de exposição modulado por agentes estatais e privados. Importante aspecto trabalhado pela crítica no campo sociológico[5] é a voluntariedade no fornecimento de informações. Somos condicionados a uma exposição permanente e contínua, seja em termos de divulgação de informações em redes sociais, seja na criação de cadastro nos diversos serviços que a tecnologia proporciona.

A obra "Vigilância Líquida" discorre como, voluntariamente, fornecemos nossos dados em troca das utopias oferecidas pela tecnologia. Os autores traçam atravessamentos entre

[2] HARCOURT, Bernard. *Exposed: Desire and disobedience in the digital age*. Londres: Harvard University Press, 2015, p. 118.

[3] FOUCAULT, Michel. *Vigiar e punir: nascimento da prisão*. Petrópolis: Vozes, 1987. Tradução: Raquel Ramalhete.

[4] DELEUZE, Gilles. *Post scriptum sobre as sociedades de controle*. Conversações: 1972-1990. Rio de Janeiro: Ed. 34, 1992, p. 221. Tradução de Peter Pál Pelba.

[5] BAUMAN, Zygmunt e LYON, David . *Vigilância Líquida.* Tradução: Carlos Alberto Medeiros. São Paulo: Zahar,2015, 1ª Edição (ebook).

a política de drones americana, como forma de invasão externa da privacidade, e a "morte do anonimato", desmantelamento interno e voluntário fomentado por pulsões da sociedade. A noção de invasão externa da privacidade ecoa na obra de Zuboff[6], quando a autora passa a tratar das práticas do *google street view*. A empresa da *google* implantou a tecnologia de mapeamento sem levar em consideração as preocupações com privacidade, construindo as próprias teses jurídicas à medida que problemas eram aventados. É um modelo de desenvolvimento que preconiza o avanço, "quebrar primeiro e perguntar depois", esse é o lema.

Os limites nebulosos entre o público e o privado em uma sociedade neoliberal apontam para uma simbiose nas práticas de vigilância. Estados fazem uso de tecnologias de vigilância elaboradas por empresas que, por sua vez, se apropriam da infraestrutura fornecida por grandes polos tecnológicos e isenções fiscais na localização de seus servidores. O poder político das grandes empresas eletrônicas exibe um cenário monopolista. Qualquer ameaça de competição é modulada pela possibilidade de fusões e aquisições[7], aumentando o espaço de ingerência de empresas singulares, o que lhes dá um aspecto omnipresente. Isto posto, é importante lembrar que, mesmo com os avanços da computação em nuvem, existe um espaço físico de armazenamento e transmissão das informações.

Este cenário expõe a corporeidade das forças econômicas de mercantilização da nossa "*cotidianeidade"*[8]. Uma sociedade guiada pela extração de valor do sujeito que não mais é visto a partir da força de trabalho, tampouco como produto, mas matéria bruta:

> Nós não somos os clientes do capitalismo de vigilância. Contudo o ditado que afirma que "se é de graça você é o produto" também não está correto. Nós somos as fontes do excedente do capitalismo: os objetos de uma inescapável operação de extração de matéria bruta. (tradução livre)[9]

A *Lex Mercatoria* apresenta-se como uma fonte tácita do direito. O espaço de modulação global de ordenamentos jurídicos por vetores econômicos implica na insuficiência de um pensamento atomizado. No meio digital, observa-se o nascimento de uma nova

---

[6] ZUBOFF, Shoshana. The age of surveillance capitalism. Nova York: Public Affairs, 2019, p. 96.

[7] Empresas como o Facebook, Google, Microsoft e Apple realizaram diversas aquisições de suas competidoras aumentando seu portifólio. Nesse sentido: LISS, Daniel. "*Today's real story: The Facebook monopoly"* in Tech Crunch, 19 de agosto de 2021. Disponível em: https://techcrunch.com/2021/08/19/todays-real-story-the-facebook-monopoly/ Acesso em 28/11/2021.

[8] Termo cunhado por Zuboff que designa as operações econômico políticas que informam o dia à dia; cf. ZUBOFF, Shoshana. *Big Other: capitalismo de vigilância e perspectivas para uma civilização de informação* in*: Tecnopolíticas da vigilância : perspectivas da margem*. Organização: Fernanda Brunoet al.] . Tradução: Heloísa Cardoso Mourão et al1. ed.. São Paulo : Boitempo, 2018, p 25.

[9] ZUBOFF, Shoshana. The age of surveillance capitalism. Nova York: Public Affairs, 2019, p. 15.

perspectiva, é a chamada *"Lex Vigilatoria*[10]*"*. Assim como a *Lex Mercatoria*, a "*Lex Vigilatoria"* obteve independência das instituições jurídicas do Estado. As políticas públicas discutidas em sede de corte constitucional europeia não contavam com espaços de debate da sociedade civil[11]; os legisladores que validam novos regulamentos estão frequentemente afastados do funcionamento real dessas tecnologias pela estrutura parlamentar de subcomissões e o processo de aprovação moroso e disperso. Assim, os parlamentares promulgam legislações sem o devido embasamento teórico necessário. A preocupação por segurança norteia a expansão tecnológica, acoplando-se ao ordenamento jurídico, na maioria das vezes, através de reforço das instituições policiais[12].

É nesse panorama jurídico político que se insere a autodeterminação informativa. A autodeterminação informativa através de seus aspectos individuais e coletivos tem, por óbvio, íntima relação com o Direito à privacidade. A legislação europeia - que inspirou a Lei geral de proteção de dados brasileira - preconiza os sistemas que são formulados privilegiando a privacidade, o chamado *privacy by design* [13]. Porém, o que se pretende apontar é uma disputa econômica pelo monopólio da privacidade. Está ocorrendo um processo de privatização do Direito à Privacidade na internet através de empresas que propagandeiam a possibilidade efetiva de ferramentas de anonimização, são as chamadas VPN (Very Private Network).

Mas como garantir a privacidade e ao mesmo tempo cumprir as exigências de armazenamento do Marco Civil e os preceitos da Lei Geral de Proteção de dados? Como garantir a liberdade em um espaço de constante monitoramento? As ferramentas que prometem ao consumidor completa anonimização parecem carecer de lastro comprobatório efetivo, como se pode observar do recente escândalo de uma das maiores empresas de VPN[14] . Em matéria Processual Penal, a afirmação de criptografia inviolável feita pelo *whatsapp* é desmantelada frente à possibilidade de recuperação de mensagens através do sistema CELLEBRITE[15] .

---

[10] MATHIESEN, Thomas. Towards a Surveillant Society: The Rise of Surveillance Systems in Europe Londres: Waterside Press, 2013, p. 165.

[11] MATHIESEN, Thomas. Towards a Surveillant Society: The Rise of Surveillance Systems in Europe Londres: Waterside Press, 2013, p. 165

[12] MATHIESEN, Thomas. Towards a Surveillant Society: The Rise of Surveillance Systems in Europe Londres: Waterside Press, 2013, p. 166.

[13] Mais sobre o tema ver CAVOUKIAN, Ann. *Respect for User Privacy – Keep it User-Centric*. Disponível em : https://www.ipc.on.ca/wp-content/uploads/resources/pbd-implement-7found-principles.pdf Acesso em 29/10/2021.

[14] NICHOLS, Shaun. *ExpressVPN stands behind CIO named in UAE hacking scandal*. In: Tech Target, 16 de setembro de 2021. Disponível em: https://www.techtarget.com/searchsecurity/news/252506801/ExpressVPN-stands-behind-CIO-named-in-UAE-hacking-scandal Acesso em 28/11/2021.

[15]FANTINATO, Giovana. *Cellebrite: conheça o software usado na investigação do caso Henry*. In: Tecmundo,

Em âmbito geral, as revelações de Snowden[16] quanto à extensão da vigilância e cooperação entre Estado e instituições privadas demarcam a penetração de uma razão econômica em matéria policial. A cooperação entre agentes policiais e judiciário estrutura uma rede de vigilância global, um "arquipélago de policiamento" [17]. A VPN é uma ferramenta que vem adquirindo popularidade, mas carece de um status de regulamentação definitivo, pois até o momento não foi promulgada a Lei Penal de dados ou elaboradas as Cláusulas padrão contratuais pela ANPD. No tópico abaixo há uma breve explicação das funcionalidades das VPNS tangenciando seus efeitos jurídico políticos. A presente pesquisa é norteada pelo método de revisão bibliográfica da literatura atual no que concerne as nuances *tecnopolíticas* da cibernética, e se insere em um estudo que pretende evocar as lacunas existentes na legislação brasileira.

1. Aspectos críticos da VPN

Primeiro, é importante delimitar como funciona uma rede privada. O VPN, ou Very Private Network, é uma ferramenta que criptografa dados. Age como um local intermediário no acesso à internet. De maneira geral, para acessar uma página na internet, o indivíduo envia as informações (pacotes) de seu endereço eletrônico (IP), através do protocolo específico da internet, para o local onde a página está hospedada. Com um VPN, seja ele gratuito ou pago, as informações são enviadas - antes de chegarem na internet - a um servidor centralizado que criptografa dados, atribuindo o endereço específico do servidor ao IP do usuário.

O VPN, de maneira geral, encobre a localização do titular dos dados. Os servidores de VPN agem como proxies para o acesso à internet. Como os dados de localização do titular estão atrelados a um servidor em determinado país, sua localização de fato não pode ser determinada. Aqui encontra-se um dos problemas centrais de governança dessa ferramenta. A maioria dos serviços de VPN não cria registros de suas atividades; alguns registram as atividades de conexão, mas não enviam as informações a terceiros. No entanto, recentes

14 de abril de 2021. Disponível em: https://www.tecmundo.com.br/software/215422-cellebrite-conheca-software-usado-investigacao-caso-henry.htm Acesso em 14/10/2021.

[16] Arquivo das denúncias de Snowden disponível em:https://theintercept.com/collections/snowden-archive/ Acesso em 28/11/2021.

[17] BIGO, Didier. *Globalized (in)Security: the Field and the Ban-opticon.* In: BIGO, Didier e TSOUKSALA, Anastassia. *Terror, Insecurity and Liberty.* Reino Unido: Routledge, 2008.

escândalos[18] demonstram que essa garantia de anonimato não é viabilizada na prática. Ao mesmo tempo ressalta-se que essa garantia não pode ser oposta à ingerência do poder público, seja a coleta de informações realizada por base em programas massivos de vigilância e suas legislações correspondentes, seja na requisição específica de ordem judicial.

Uma maneira interessante de entender os VPNs é a classificação proposta por Heesmbergen e Molnar[19] através do termo *"boundary objects*", ou objetos limite. Esses objetos são classificados, a partir da categorização de Star[20], como instrumentos utilizados por pessoas em relação a seus próprios campos práticos. A criptografia inerente a esses processos envolve uma fluidez de conhecimento, que passa desde um estágio que se pretende puramente técnico, tratando do saber matemático envolvido nos processos de anonimização, até os paradigmas legais que determinam os limites dessa tecnologia e as maneiras de governá-la. A proposta dos pesquisadores, mais do que a interpretação do que significa o uso prático do VPN, procura entender os efeitos políticos de seu uso:

> Nosso foco em particular é na ecologia experienciada por usuários que vem antes da experiência dentro do aplicativo. Registros simbólicos e representativos ligados a experiencia do usuário de aprendizado e na decisão de utilização de um VPN apresentam uma rica fonte de material para mapear as facetas deste objeto limite [21] (Tradução Livre)

Os pesquisadores delimitam três pontos de inflexão no estudo das VPNs. O primeiro se relaciona ao objeto de estudo em si. Trata-se de uma visão voltada para a ecologia da utilização desses sistemas ao revés da experiência de uso de determinada aplicação ou dos aspectos econômicos envolvidos em seu uso. O segundo é a percepção de um ímpeto das VPNs

---

[18] Para um detalhamento do recente escândalo de VPNS ver: BODE, Karl. *Latest VPN Security Scandals Show (Yet Again) That VPNs Aren't A Panacea*. In: Techdirt, 22 de julho de 2020. Disponível em: https://www.techdirt.com/articles/20200719/11115744928/latest-vpn-security-scandals-show-yet-again-that-vpns-arent-panacea.shtml Acesso em 28/10/2021. Ver também: Gadgets 360 Newsdesk (sem autor mencionado) *After ExpressVPN CIO Named in UAE Surveillance Scandal; Edward Snowden Says Stop Using It*. In: Gadgets 360, 18 de setembro de 2021. Disponível em: https://gadgets.ndtv.com/internet/news/expressvpn-hacking-scandal-uae-edward-snoden-tweet-data-privacy-2545125 Acesso em 29/10/2021

[19] HEEMSBERGEN, Luke e MOLNAR, Adam. VPNs as boundary objects of the internet: (mis)trust in the translation(s). In Revista eletrônica: Internet Policy Review, volume 9 edição 4. 21 de outubro de 2020 disponível em: https://policyreview.info/articles/analysis/vpns-boundary-objects-internet-mistrust-translations Acesso em 28/11/2021.

[20] STAR, Leigh. *This is not a boundary object: Reflections on the origin of a concept*. In: Science, Technology, & Human Values, 35(5), 601–617. Disponível em: https://doi.org/10.1177/016224391037762 Acesso em 29/10/2021.

[21] HEEMSBERGEN, Luke e MOLNAR, Adam. *VPNs as boundary objects of the internet: (mis)trust in the translation(s*). In: Internet Policy Review, volume 9, edição 4. 21 de outubro de 2020. Disponível em: https://policyreview.info/articles/analysis/vpns-boundary-objects-internet-mistrust-translations Acesso em 28/11/2021.

de se tornarem parte da estrutura da internet padrão, e não mais uma ferramenta a ser adicionada. A estrutura se assemelha à adoção massiva do novo padrão de conexão de internet, o chamado HTTPS. Conforme delimitam os pesquisadores, a utilização do protocolo de segurança se tornou uma prática comum após as revelações de Snowden.

O terceiro ponto, a experiência do usuário, apresenta apenas uma das facetas que definem o objeto limite. Enquanto a experiência do usuário importa na caracterização do objeto, não o define. O foco dos pesquisadores foi tentar delimitar o contexto de uso dessas ferramentas e as relações que ele implica no espaço cibernético.

A pesquisa concluiu que há duas experiências por excelência no contato de usuário com o mundo das VPNs. A primeira trata da solicitação de produtos através de buscas da internet diretamente nas empresas de VPN, e a segunda cuida do acesso a sites agregadores de diversos produtos de VPN que exibem uma espécie de ranking desses serviços.

Percebeu-se que uma das motivações para o uso casual dos VPNs é atrelada às preocupações de segurança e privacidade. De maneira desproporcional, tal discurso tem uma posição hegemônica. Esses protocolos de redes privadas, ou melhor, as informações exibidas sobre eles, passam ao largo de uma definição técnica especificada dos serviços que provêem. O discurso é centrado em torno da propaganda. Os produtos são comumente diferenciados através de parâmetros voltados ao consumidor final, como velocidade, facilidade de uso e disponibilidade de recursos de atendimento ao cliente.

Ao mesmo tempo, no viés da ideia de Pasquale[22], vê-se que os algoritmos funcionam como verdadeiras caixas pretas. Esses algoritmos utilizados para a garantia da privacidade, ou as medidas de segurança empreendidas por essas empresas para viabilizar a privacidade, não são explicitadas. As tecnologias de VPN parecem nos fornecer uma visão utópica de liberdade frente ao controle e à vigilância de grandes empresas e aparelhos estatais, mas não substanciam tais informações a partir de uma delimitação técnica especificada.

A opacidade, conforme Doneda e Almeida[23], é uma marca distintiva desses algoritmos. Por um lado, há uma questão técnica, voltada para a dificuldade em decodificar os resultados derivados dos processos algorítmicos. Por outro, há razões políticas para a manutenção do algoritmo nesse status, os autores Doneda e Almeida[24] suscitam a questão da

[22] PASQUALE, Frank. The Black Box Society. *The Secret Algorithms That Control Money and Information.* Londres: Harvard University Press, 2015.

[23] ALMEIDA, Virgílio e DONEDA, Danilo. *O que é a governança de algoritmos?* In: *Tecnopolíticas da vigilância: perspectivas da margem*. São Paulo: Boitempo, 2018, p. 141. Organização: Fernanda Bruno et al.

[24] ALMEIDA, Virgílio e DONEDA, Danilo. *O que é a governança de algoritmos?* In: *Tecnopolíticas da*

concorrência mercadológica como um fator importante. No caso das VPNs, pode-se argumentar que por questões de segurança e privacidade os algoritmos atinentes ao processo de criptografia e anonimização também são munidos de uma opacidade justificável.

Em todo caso, a governança algorítmica, definida por Doneda e Almeida[25] , através da necessidade de "priorizar a responsabilização, a transparência e as garantias técnicas", é o fenômeno geral do qual tratamos. Há uma carga moral e jurídica atrelada às tecnologias algorítmicas e um suposto caráter de neutralidade na realização de objetivos pré-definidos supostamente despidos de um caráter político. Durante a pandemia do COVID-19, a liberdade conferida à vigilância dos Estados sob a justificativa de um controle epidemiológico já tem gerado diversos problemas.[26] A instalação de uma razão algorítmica, que vê na tecnologia uma panaceia, dá a tônica de um "*solucionismo tecnológico*"[27], e tem assumido cada vez mais força.

Há uma sedimentação do entendimento que apregoa uma suposta eficiência intrínseca, incorruptível e neutra da razão algorítmica. As soluções computacionais, fundadas em critérios aparentemente técnicos, são estratégias de governo. São estratégias de legitimação que pleiteiam a força de um regime de *veridicção* através de dados, como meio que se pretende organizador da política. É também um processo de valorização da estatística como tática de intervenção social configurada a partir da chamada "virada atuarial"[28]. Para além de uma visão pessimista *orwelliana*, deve-se atentar para a fragilidade e novidade histórica dessas práticas de controle. Mesmo que se apresentem como tendo uma composição verticalizada e imutável, as ferramentas do universo tecnológico constituem espaços de disputa permanente.

O debate acerca dos VPNs não se resume a uma mercantilização da privacidade, mas abarca também a possibilidade de resistência. O VPN pode emergir como uma nova ferramenta que não tem um caráter intrínseco voltado para o abuso de direito. Na revolução

vigilância: perspectivas da margem. São Paulo: Boitempo, 2018, p 143. Organização: Fernanda Bruno et al.

[25] ALMEIDA, Virgílio e DONEDA, Danilo. *O que é a governança de algoritmos?* In: *Tecnopolíticas da vigilância: perspectivas da margem*. São Paulo: Boitempo, 2018, p 145. Organização: Fernanda Bruno et al.

[26] É o caso de Singapura na propagação de um aplicativo de combate epidemiológico. Inicialmente o Estado afirmou que a finalidade dos dados seria restrita ao combate a pandemia, no entanto, esses dados foram compartilhados com agências policiais. Neste sentido, ILLMER, Andreas. 'Singapore reveals Covid privacy data available to police". BBC News, 5 de janeiro de 2021. Disponível em: https://www.bbc.com/news/world-asia-55541001 Acesso em: 26/10/2021

[27] AMARAL, Augusto Jobim e SALLES, Eduardo Baldisserra. *Pandemia, vigilância e os perigos do Solucionismo tecnológico*. In: Ciências Criminais e Covid 19. São Paulo: Tirant Lo Blanch, 2020, p. 154. Org: Nereu José Giacomolli.

[28] HARCOURT, Bernard. *The pull of prediction: Distorting our concepctions of Just Punishment*. In *Algoritarismos.* Tirant Lo Blanch: São Paulo, 2020, p 370. Org: Jesus Sabariego; Augusto Jobim do Amaral; Eduardo Badissera Carvalho.

iraniana[29] o VPN foi uma ferramenta de resistência ao despotismo do regime, sendo utilizado pelos manifestantes para a divulgação segura de abusos contra os Direitos Humanos. A história do controle informacional não é recente, os instrumentos são. A cronologia desse controle pode ser visualizada, por exemplo, na sedimentação do Estado e de suas funções administrativas[30].

O desconhecimento geral sobre o funcionamento dessas plataformas nos leva a uma impotência de difícil superação, ainda mais quando se trata de VPN. Segundo Hemsbergen e Molnar[31], a maioria das empresas de VPN afirmam que não armazenam dados dos usuários, outras (com base em dados fornecidos em investigações policiais) informam que mantêm apenas dados referentes a atividades básicas como logs de atividade e horários de utilização. A garantia de que esses dados não são armazenados é impossível de ser verificada pelos usuários; a confiança cega nos algoritmos e na proteção que eles proveem passa a ser um dos vetores de estruturação de uma nova forma de vida. Segundo AMARAL[32], vivemos num cenário "algoritário", definido como:

> Um conjunto multidimensional de práticas políticas reatualizáveis por diversos agenciamentos, práticas estas dispostas tecnologicamente a sequestrar o ritmo vital que faz vibrar qualquer sentido, ou seja, modos de um dispositivo ´dado´ a informar, planificar funções repetíveis e a conformar futuros prováveis sob lógicas de dor padronizadamente aprofundadas.

A delimitação de um espaço cosmopolítico na implementação de novas tecnologias demonstra que a utilização em si do VPN, a experiencia do usuário, a possibilidade ofertada de resistência e a disputa mercadológica subsidiam o entendimento geral de utilização dessas plataformas. Para o contexto brasileiro, no presente esforço, importa o limite de ingerência do poder público no controle dessa ferramenta e a existência, ainda tímida, de regulamentação específica, tema a ser tratado no tópico seguinte.

---

[29] BOWEN, Kyle. Marchant, James. *Revolution decoded: Internet Censorship in IRAN: Preventative, Interceptive and reactive*. Small Media UK, 2015. Disponível em: https://smallmedia.org.uk/revolutiondecoded/a/RevolutionDecoded.pdf Acesso em 25/11/2021.

[30] Para mais sobre o tema da incorporação do Direito administrativo na razão de Estado ver: FOUCAULT, Michel. *Sociedade Punitiva*. São Paulo: WMF Martins Fontes, 2015, p 215. Tradução Ivone C Benedetti. Ver também: FOUCAULT, Michel. *Teorias e instituições Penais*. São Paulo: WMF. Martins fontes, 2020, p. 156. Tradução Rosemary Costhek Abílio

[31] HEEMSBERGEN, Luke e MOLNAR, Adam. *VPNs as boundary objects of the internet: (mis)trust in the translation(s*). In: Internet Policy Review, volume 9, edição 4. 21 de outubro de 2020. Disponível em: https://policyreview.info/articles/analysis/vpns-boundary-objects-internet-mistrust-translations Acesso em 28/11/2021.

[32] AMARAL, Augusto Jobim do. *Prólogo.* In: *Algoritarismos*. Tirant Lo Blanch: São Paulo, 2020, p 10. Organização: Jesus Sabariego et al.

2. Marco Civil da Internet e VPN

Na linha que postula Lemos e Souza[33], destaca-se a importância do processo dialético de construção do Marco Civil da internet, iniciado em 2007 e aprovado em 2014, como culminação de diálogo aberto com a sociedade civil. Em meio ao ordenamento jurídico brasileiro, nos deparamos com uma pergunta central: podem as companhias provedoras de serviço de VPN opor sua garantia de anonimização, sua intencionalidade no desconhecimento tecnicamente estruturado dos dados de sujeitos que fazem uso de seus serviços, às requisições judiciais emanadas do poder público? A legislação brasileira exige a capacidade técnica de identificação dos usuários do serviço ou poderia uma empresa alegar que sua infraestrutura técnica impede o conhecimento e pormenorização dos serviços utilizados por seus usuários? Quais problemas surgem na ordem do Direito Internacional?

O debate aqui vai para além da colisão entre os Direitos da personalidade e a Liberdade de expressão. Trata da possibilidade concreta da efetivação da privacidade como condição de possibilidade de manifestação de opiniões políticas e artísticas assim como a concretude de um Direito Fundamental à proteção de dados[34]. Para tentar responder os questionamentos suscitados utilizar-se-á as conclusões obtidas do Marco Civil da Internet e da Lei Geral de Proteção de dados e a doutrina que as atravessa.

O VPN é classificado como provedor de conexão, já que sua função se adequa à definição do artigo 5º inc. V do Marco Civil que explicita a conexão da internet como "a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP". Aqui encontramos a primeira questão problemática. O VPN funciona conectando o endereço de IP a um servidor que se encontra em qualquer parte do mundo. O registro de conexão, exigência do artigo 13 do Marco Civil, indicará que o endereço de IP do titular de dados se conectou com o servidor da empresa que

---

[33] SOUZA, Carlos Affonso; LEMOS, Ronaldo. *Marco Civil da Internet: Construção e Aplicação*. Disponível em: https://itsrio.org/wp-content/uploads/2017/02/marco_civil_construcao_aplicacao.pdf p. 14 Acesso em: 23/09/2021.

[34] O caráter fundamental do direito à proteção de dados já é amplamente reconhecido pela doutrina. Neste sentido SARLET, Ingo. *Fundamentos Constitucionais: O direito fundamental à proteção de dados*. In: BIONI, Bruno (coordenador Executivo) *Tratado de proteção de dados Pessoais*. Forense: Rio de Janeiro, 2021, Ebook, pos 300; SARLET, Ingo. *A eficácia dos direitos fundamentais: Uma teoria geral dos direitos fundamentais na Perspectiva Constitucional*. Livraria do Advogado: Porto Alegre, 12ª edição, 2015. SARLET, Ingo "Proteção de dados pessoais como Direito Fundamental na constituição Federal Brasileira de 1988: Contributo para a construção de uma dogmática constitucionalmente adequada" Belo Horizonte, 2020. Revista: Direitos Fundamentais e justiça, ano 14, n 42, p 179-218, jan-jun 2020; SARLET, Ingo "O conceito de direitos fundamentais na Constituição Federal de 1988" 27 de fevereiro de 2015. Disponível em: https://www.conjur.com.br/2015-fev-27/direitos-fundamentais-conceito-direitos-fundamentais-constituicao-federal-1988 Acesso em: 25/05/2021

oferece VPN; no entanto, não é claro, diante da variedade de serviços, se na prática todas as empresas se atêm à exigência de coleta de dados de registro ou guarda destes pelo período de um ano.

As obrigações do Poder Público, para além do Direito Constitucional e Direito Internacional dos Direitos Humanos, perpassam pela observância da gama de princípios consubstanciados pelos artigos 2º e 3º do Marco Civil. No caso da VPN, merece especial destaque o artigo 7º. Os incisos I ao III do art. 7º tratam especificamente do dever de inviolabilidade de dados, mas no inciso VI vemos que a legislação esbarra nos problemas atinentes ao algoritmo de anonimização levantados no tópico anterior. Narra o inciso VI:

> Informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade.

Como poderia a empresa de VPN detalhar a maneira de anonimização dos dados sem colocar em risco a própria inviolabilidade destes dados? A questão permanece em aberto.

Ao mesmo tempo, o artigo 10 da Lei 12965 de 2014 (Marco Civil da Internet) exige a guarda, registro e manutenção dos dados de conexão. Os serviços de VPN que não mantêm registro de conexão de seus usuários, pela própria natureza do seu serviço, estariam impossibilitados de fornecerem essas informações. A situação gera o risco da imputação, aos responsáveis, do crime Desobediência (art. 330 do CP) diante da impossibilidade do fornecimento dessas informações. A especificidade, dentro do próprio campo das VPNs, nos leva a questionar a legalidade de serviços que não realizam esse controle. É evidenciada desse modo a não compatibilidade, ou a ilegalidade, dos serviços de anonimização que não realizam o registro de dados de conexão.

A situação se agudiza quando se leva em conta a disparidade de legislações internacionais. O fato destes servidores estarem localizados em outros países traz a necessidade de representação jurídica dessas empresas em âmbito nacional visto que a exigência positivada pelo artigo 8º inciso II do Marco Civil evoca a necessidade de adoção do foro brasileiro para a resolução de controvérsias.

A extra-territorialidade do processo de anonimização também comporta problemas práticos levantados frente ao artigo 11 do Marco Civil. Narra o artigo que:

> Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser

> obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

A controvérsia que surge sobre a incidência da legislação brasileira é resolvida pelo parágrafo 2º do mesmo artigo. Para determinar a jurisdição adequada aos serviços de VPN- já que o processo de anonimização, ou o redirecionamento da conexão ao servidor, se localiza em território estrangeiro- é necessário levar em conta se este constitui "oferta de serviço ao público brasileiro". Resta evidente a aplicabilidade irrestrita da legislação brasileira a esses serviços, já que de fato o serviço de VPN constitui oferta de serviço ao público brasileiro.

Pelo exposto, é aplicável o artigo 13 do Marco Civil. O artigo positiva a necessidade de guarda e manutenção dos registros de conexão e seu fornecimento incontroverso quando há a requisição judicial precedida dos elementos necessários de identificação e especificando sua finalidade. O requerimento de dados também deve respeitar as garantias constitucionais e aquelas previstas no artigo 22 caput e incisos do Marco Civil, o que novamente colocaria em xeque os serviços de VPN que não mantêm registros de conexão. Portanto, podemos concluir que a proibição ou liberação de Serviços de VPN está subordinada à manutenção desses registros. Aquelas empresas que alegam não manter os registros de conexão não estariam de acordo com a legislação vigente.

Essa conclusão nos traz outro problema de ordem prática. Como foi posto, os VPNs não são provedores de aplicação; no entanto, ao mascarar o endereço eletrônico, acabam por impedir que os provedores de aplicação identifiquem determinadas ações dos sujeitos que fazem uso dessa anonimização. Assim, permanece em suspenso se os serviços de VPN estariam adstritos a uma responsabilização específica diante da remoção de conteúdo por ordem Judicial. Para identificar um sujeito que realizou uma postagem racista em uma rede social através de uma VPN, por exemplo, haveria a necessidade de compatibilização dos registros de conexão e dos registros de acesso aos provedores de aplicação. A questão esbarra na própria vedação positivada pelo artigo 14, visto que os provedores de conexão não podem guardar os registros de acesso a aplicações.

Cabe, ainda, valorar o vetor jurisprudencial que concerne à dita "terceira onda[35]" de interpretação do Marco Civil ilustrada pela posição do ministro Ricardo Villas Boas Cueva. Em agravo no Recurso Especial 917.162/SP[36], de 1º de setembro de 2016, pode-se observar a

[35] MUNIZ, Mariana. *A terceira onda de interpretação do Marco Civil no STJ*. In: JOTA, 17 de Julho de 2017. Disponível em: https://www.jota.info/justica/a-terceira-onda-de-interpretacao-do-marco-civil-no-stj-17072017 Acesso em 28/11/2021.

[36] BRASIL. Superior Tribunal de Justiça. Agravo no Recurso Especial 917.162/SP. Relator: Min. Ricardo Villas

opção por essa linha, visto que a terceira onda é aquela interpretação que afasta a responsabilidade do provedor na avaliação de ofensas em virtude da subjetividade que comportam. Especificamente no que diz respeito à remoção de conteúdo, essas decisões não podem servir de analogia para a caracterização da responsabilização das empresas de VPN, pois à responsabilização de provedores de conexão não se aplicariam as exigências do artigo 19 do Marco Civil já que os VPNs não são provedores de aplicações.

A questão é teórica e técnica, impondo à cogente necessidade de diálogo entre o discurso jurídico, a vontade da população dentro de um Estado Democrático de Direito e os avanços técnicos. O Marco Civil pode sanar algumas questões de maneira superficial, mas cabe à jurisprudência e à prática do Direito verificar como pode funcionar a ingerência do Estado nos casos de tratamento de dados por empresas de VPN.

2.1 Lei Geral de Proteção de dados e VPN.

Sucintamente, pode-se dizer que a Lei Geral de Proteção de Dados tem forte influência da Lei europeia de Proteção de dados. Assim como a Lei europeia, a Lei brasileira não trata da proteção e obrigação do fornecimento de dados em matéria penal.[37]

A autodeterminação informativa é o primado discursivo geral que orienta a Lei Geral de Proteção de dados. O conceito pode ser classificado, na sua dimensão individual, como "o direito de cada indivíduo poder controlar e determinar o acesso e o uso de seus dados pessoais"[38]. Já a dimensão coletiva elege a autodeterminação informativa, cf. Sarlet, como garantidora de uma "ordem comunicacional livre"[39]. Vê-se que a autodeterminação informativa é um direito que comporta dimensões intersubjetivas e deveres de ação e omissão do poder público em uma relação dialética. A autodeterminação informativa está positivada no art. 2º da Lei Geral de proteção de dados.

Devemos nos atentar à LGPD quando tratamos de processos de anonimização. Em primeiro lugar, sob uma perspectiva supraindividual no que toca os limites conferidos ao poder

Boas Cueva. Data: 1 de setembro de 2016.

[37] BRASIL. Artigo 4º inciso III alínea da Lei 13.709 de 14 de agosto de 2018. *Lei Geral de Proteção de Dados.*

[38] CANOTILHO, JJ Gomes. *Direito Constitucional e Teoria da Constituição.* Coimbra: Ed. Almedina, 2003, p. 233.

[39] SARLET, Ingo. *Proteção de dados pessoais como Direito Fundamental na constituição Federal Brasileira de 1988: Contributo para a construção de uma dogmática constitucionalmente adequada.* Belo Horizonte, 2020, p 190. Revista: Direitos Fundamentais e justiça, ano 14, n 42, p 179-218, jan-jun 2020..

público na coleta destes dados. Em segundo, ao interpretar os limites conferidos aos indivíduos (titulares de dados) que modulam as possibilidades de manutenção da privacidade num espaço digital. A aplicabilidade da Lei é garantida pelo inciso II do artigo 3º e parágrafo 1º do mesmo artigo. No caso dos VPNs, os dados, mesmo que efetivamente não tenham sido coletados em território nacional, passam a ser entendidos desta forma, pois o titular dos dados está em território nacional no momento da coleta.

É no artigo 6º, IV e 9º II que encontramos um indicativo de proteção ao algoritmo que relativiza os Direitos Individuais, fortalecendo a perpetuação do desconhecimento do funcionamento desses sistemas e prejudicando a concretização do dever de uma evidente finalidade. Narra o artigo:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: VI - transparência: 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**. (meu grifo).

O artigo 9º explicita:

> Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: II - forma e duração do tratamento, **observados os segredos comercial e industrial** (meu grifo)

Ao introduzir a ressalva quanto à observação dos segredos comercial e industrial, o legislador deixa os direitos dos sujeitos sobre seus dados, as empresas de VPN e a própria ingerência do poder público numa situação de vagueza. Ora, a atividade fim dessas empresas é justamente fornecer um algoritmo de criptografia que consiga trazer privacidade dentro da rede ao mesmo tempo que tem o dever de informar seus processos. No entanto, a abertura conferida às empresas pelo potencial de qualificar seus processos como segredos comerciais ou industriais deixa o titular dos dados numa posição de vulnerabilidade, pois os processos específicos de anonimização de seus dados não são esclarecidos, colocando em risco o dever de atenção à uma evidente finalidade.

Em relação às possibilidades de tratamento de dados pelo poder público, narra o artigo 7 inciso VI da LGPD que os dados podem ser requisitados "para o exercício regular de direitos em processo judicial, administrativo ou arbitral". Esse fornecimento pode ser prejudicado pela peculiar natureza do serviço. As empresas estão restritas pela própria opção limítrofe de abstenção de identificação no tratamento de dados. De modo transversal os VPNs acabam por impossibilitar de maneira bifronte o fornecimento de acesso a provedores de conteúdo. Por um lado, pela exigência legal do Marco Civil de abstenção dos provedores de

conexão no monitoramento de acesso a aplicativos e, por outro, ao impedir que os provedores de aplicativos consigam determinar a identidade do titular de dados. Vejamos, quando há a requisição de determinados dados a um provedor de aplicativos, e o endereço eletrônico suscitado indica endereço eletrônico geral fornecido pela VPN, não é claro se essas empresas conseguirão ou mesmo se elas têm meios técnicos para especificar o titular de dados específico. Ou seja, a própria razão de ser da VPN, virtualmente, estaria impedindo a possibilidade de fornecimento de registros de acesso a conteúdo de aplicativos.

Voltando às questões gerais, diversos autores [40] tem discutido a aparente contradição que permeia a questão aqui tratada. Uma aparente contradição entre a privacidade e o interesse público entendido de maneira ampla. A contradição é aparente, pois a questão perpassa pela necessidade de entendimento de uma dimensão da privacidade que não se resume ao sujeito, que vá além de uma perspectiva individual. Conforme Wimmer[41], trata-se de um esforço de superação da percepção de interesse público e privacidade como antípodas, postulando uma concepção dessas noções como "elementos que se reforçam mutuamente". Neste cenário - que conjuga a privacidade e interesse público- esses princípios passam a integrar uma relação mais ampla, alicerçada na obrigação do Estado em garantir a materialização da aplicabilidade imediata de Direitos Fundamentais.

Há, ainda, mais uma dimensão a ser evocada: a regulamentação da transferência internacional de dados. Essa transferência, como leciona Mascarenhas [42], pode ocorrer de maneira direta e indireta. A transferência direta, como evidencia o nome, é a relação de tratamento de dados em que a empresa possui contrato direto com o titular, já a hipótese de transferência indireta cuida da situação em que o tratamento de dados pessoais se justifica a partir de uma terceira empresa. É importante destacar que, no cenário delimitado pela LGPD, as empresas de VPN funcionam como controladoras pois, como narra Leonardi[43]:

> Toda vez que uma empresa efetua o tratamento de dados pessoais decidindo as maneiras e as finalidades desse tratamento, ela se enquadra na definição de controlador(...) pois é a pessoa jurídica a quem competem as decisões referentes ao

[40] Sobre o tema destaca-se: SARLET, Ingo (a). Fundamentos Constitucionais: *O direito fundamental à proteção de dados*. In: BIONI, Bruno (coordenador Executivo). *Tratado de proteção de dados Pessoais*. Rio de Janeiro: Forense, 2021, p 48; WIMMER, Miriam. *O regime jurídico do tratamento de dados pessoais pelo Poder público*. In: Tratado de proteção de dados Pessoais. Rio de Janeiro: Forense, 2021, p 288; SOLOVE, Daniel. *Understanding Privacy.* Londres: Harvard University Press, 2008, p. 87.

[41] WIMMER, Miriam. *O regime jurídico do tratamento de dados pessoais pelo Poder público*". In: Tratado de proteção de dados Pessoais. Forense: Rio de Janeiro, 2021, p. 289.

[42] MASCARENHAS, Fernanda. *O regime de transferência Internacional de dados da LGPD: Delineando as opções regulatórias em jogo.* In: Tratado de proteção de dados Pessoais" Forense: Rio de Janeiro, 2021, p. 313

[43] LEONARDI, Marcel. *Transferência internacional de dados pessoais*. In: *Tratado de proteção de dados Pessoais.* Rio de Janeiro: Forense, 2021, p. 301.

tratamento

A LGPD, a partir de seu artigo 33, inc. I, a exemplo da legislação europeia, condiciona a transferência internacional de dados à existência de um regime de proteção similar àquele previsto na Lei brasileira. A análise da comparabilidade entre as duas legislações cabe à Autoridade Nacional de Proteção de Dados. Sua avaliação deverá levar em conta o disposto nos incisos do artigo 34 da LGPD:

> Art. 34. O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do caput do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração:
> I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional; II - a natureza dos dados; III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei; IV - a adoção de medidas de segurança previstas em regulamento; V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e VI - outras circunstâncias específicas relativas à transferência.

A requisição realizada por ordem judicial recai sobre o âmbito da cooperação jurídica internacional conforme inciso III do artigo 33. Deve assim o juiz valorar se o interesse público no caso concreto é proporcional à fragilização da dimensão subjetiva da autodeterminação informativa. No caso específico das VPNs, no momento presente, parece inexato afirmar que a transferência de dados ocorreria pelas chamadas cláusulas padrão contratuais. A elaboração de seu conteúdo é de competência da ANPD[44]. No entanto, até o momento, essas cláusulas contratuais não foram elaboradas, estando previstas para o primeiro semestre de 2022[45]. A solução das questões aventadas caminha no sentido da necessidade de um multissetorialismo, cf. Aranha:

> A participação no Comitê (com garantia de assento) do setor privado, da sociedade civil organizada e da comunidade técnica garantiria que as questões relacionadas entre direito e tecnologia tivessem uma visão multidisciplinar. A LGPD e o Marco Civil da Internet (Lei 12.485/2014) apontam para essa composição, com o Conselho Nacional de Proteção de Dados e Privacidade (CNPD) e o Comitê Gestor da Internet (CGI.Br)[46].

Note-se ainda que a Lei atribui um extenso rol de competências à autoridade nacional de proteção de dados. Ainda que condicionada às exigências presentes na LGPD, a atuação da

---

[44] BRASIL. Autoridade Nacional de Proteção de Dados. Portaria 1º, de 8 de março de 2021

[45] Portal eletrônico da Autoridade nacional de proteção de dados(sem menção de autor). "ANPD participa do II Diálogo Digital Brasil - Reino Unido 2021" publicado em 9/04/2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-participa-do-ii-dialogo-digital-brasil-reino-unido-2021 Acesso em: 25/11/2021.

[46] ARANHA, Estela. *Elaboração de parecer sobre a legalidade dos Decretos nº 10.046/2019 e 10.047/2019 em face das normas que disciplinam os direitos fundamentais à proteção de dados e à privacidade no ordenamento jurídico brasileiro*. p.34 Disponível em: https://www.oabrj.org.br/sites/default/files/parecer_final_rev._30_jan_2020_lucia_dec._10.046-_comissao_prot_de_dados.docx.pdf Acesso em 23/08/2021.

autoridade nacional de proteção de dados e seus poderes atinentes ao tratamento de dados por empresas de VPN deve ser conduzida de maneira ampla frente à sociedade civil. As decisões de cessação e proibição de transferência de dados devem possuir clara motivação, indicando as razões específicas da decisão tomada. Por fim, diante da atribuição de competências conferida à autoridade nacional de proteção de dados, resta evidente que apenas através da publicização de seus atos administrativos motivados e da incorporação do multissetorialismo é que poderemos afirmar a compatibilidade de empresas de VPN internacionais com a legislação interna.

3. Conclusão.

Como observado inicialmente, há uma disputa econômica pelo monopólio da privacidade travada entre as empresas de VPN. Conforme pesquisa técnica suscitada, é perceptível um ímpeto dos usuários na busca de VPNs consubstanciados por preocupações de segurança e privacidade. Paralelamente foi possível notar que os algoritmos que compõem os processos de anonimização possuem uma opacidade justificada pela concorrência intrínseca às figuras de propriedade intelectual. Ao mesmo tempo, constata-se que o uso das VPNs não se resume a uma mercantilização da privacidade, mas abarca também a possibilidade de resistência política.

Conforme disciplina o MCI podemos concluir que a proibição ou liberação de Serviços de VPN está subordinada à manutenção dos registros de dados de acesso. Aquelas empresas que alegam não manter os registros de conexão não estariam de acordo com a legislação vigente. Na linha explicitada pela LGDP, quando se introduz a ressalva quanto à observação dos segredos comercial e industrial, o legislador deixa os direitos dos titulares de dados, as empresas de VPN e a própria ingerência do poder público numa situação de vagueza. De modo transversal, os VPNs acabam por impossibilitar de maneira bifronte o fornecimento de acesso a provedores de conteúdo. Por um lado, pela exigência legal do Marco Civil de abstenção dos provedores de conexão no monitoramento de acesso a aplicativos e, por outro, ao impedir que os provedores de aplicativos consigam determinar a identidade do titular de dados.

Referências.

ALMEIDA, Virgílio e DONEDA, Danilo. *O que é a governança de algoritmos?* In: *Tecnopolíticas da vigilância: perspectivas da margem*. São Paulo: Boitempo, 2018, p. 141. Organização: Fernanda Bruno et al.

AMARAL, Augusto Jobim e SALLES, Eduardo Baldisserra. *Pandemia, vigilância e os perigos do Solucionismo tecnológico*. In: Ciências Criminais e Covid 19. São Paulo: Tirant Lo Blanch, 2020, p 154. Org por: Nereu José Giacomolli

_____, Augusto Jobim do. *Prólogo.* In: *Algoritarismos*. Tirant Lo Blanch: São Paulo, 2020, p 10. Organização: Jesus Sabariego et al.

ARANHA, Estela. *Elaboração de parecer sobre a legalidade dos Decretos nº 10.046/2019 e 10.047/2019 em face das normas que disciplinam os direitos fundamentais à proteção de dados e à privacidade no ordenamento jurídico brasileiro*. Disponível em: https://www.oabrj.org.br/sites/default/files/parecer_final_rev._30_jan_2020_lucia_dec._10.046-_comissao_prot_de_dados.docx.pdf. Acesso em 23/08/2021.

BAUMAN, Zygmunt e LYON, David . *Vigilância Líquida.* Tradução: Carlos Alberto Medeiros. São Paulo: Zahar,2015, 1ª Edição (ebook).

BIGO, Didier. *Globalized (in)Security: the Field and the Ban-opticon* in BIGO, Didier e TSOUKSALA, Anastassia. "Terror, Insecurity and Liberty" Reino Unido: Routledge, 2008.

BOWEN, Kyle. Marchant, James. *Revolution decoded : Internet Censorship in IRAN: Preventative, Interceptive and reactive*. Small Media UK, 2015. Disponível em: https://smallmedia.org.uk/revolutiondecoded/a/RevolutionDecoded.pdf. Acesso em 25/11/2021.

BRASIL. Superior Tribunal de Justiça. Agravo no Recurso Especial 917.162/SP. Relator: Min. Ricardo Villas Boas Cueva. Data: 1 de setembro de 2016.

BRASIL. Autoridade Nacional de Proteção de Dados. Portaria 1º, de 8 de março de 2021
CAVOUKIAN, Ann. *Respect for User Privacy – Keep it User-Centric.* Disponível em : https://www.ipc.on.ca/wp-content/uploads/resources/pbd-implement-7found-principles.pdf Acesso em 29/10/2021.

BODE, Karl. *Latest VPN Security Scandals Show (Yet Again) That VPNs Aren't A Panacea*. In: Techdirt, 22 de julho de 2020. Disponível em: https://www.techdirt.com/articles/20200719/11115744928/latest-vpn-security-scandals-show-yet-again-that-vpns-arent-panacea.shtml . Acesso em 28/10/2021.

CANOTILHO, JJ Gomes. *Direito Constitucional e Teoria da Constituição.* Coimbra: Ed. Almedina, 2003.

DELEUZE, Gilles. *Post scriptum sobre as sociedades de controle.* Conversações: 1972-1990. Rio de Janeiro: Ed. 34, 1992, p. 221. Tradução de Peter Pál Pelba.

FANTINATO, Giovana. *Cellebrite: conheça o software usado na investigação do caso Henry*. In: Tecmundo, 14 de abril de 2021. Disponível em: https://www.tecmundo.com.br/software/215422-cellebrite-conheca-software-usado-investigacao-caso-henry.htm. Acesso em 14/10/2021.

FOUCAULT, Michel. *Vigiar e punir: nascimento da prisão*. Petrópolis: Vozes, 1987. Tradução: Raquel Ramalhete.

_____, Michel. *Sociedade Punitiva*. São Paulo: WMF Martins Fontes, 2015. Tradução Ivone C Benedetti.

_____, Michel. *Teorias e instituições Penais*. São Paulo: WMF. Martins fontes, 2020.Tradução Rosemary Costhek Abílio

Gadgets 360 Newsdesk (sem autor mencionado) *After ExpressVPN CIO Named in UAE Surveillance Scandal; Edward Snowden Says Stop Using It*. In: Gadgets 360, 18 de setembro de 2021. Disponível em: https://gadgets.ndtv.com/internet/news/expressvpn-hacking-scandal-uae-edward-snoden-tweet-data-privacy-2545125. Acesso em 29/10/2021.

HARCOURT, Bernard. *Exposed: Desire and disobedience in the digital age*. Londres: Harvard University Press, 2015.

_____, Bernard. *The pull of prediction: Distorting our concepctions of Just Punishment*. In *Algoritarismos*. Tirant Lo Blanch: São Paulo, 2020. Org: Jesus Sabariego; Augusto Jobim do Amaral; Eduardo Badissera Carvalho.

HEEMSBERGEN, Luke e MOLNAR, Adam. *VPNs as boundary objects of the internet: (mis)trust in the translation(s)*. In Revista eletrônica: Internet Policy Review, volume 9 edição 4. 21 de outubro de 2020 disponível em: https://policyreview.info/articles/analysis/vpns-boundary-objects-internet-mistrust-translations. Acesso em 28/11/2021.

ILLMER, Andreas. 'Singapore reveals Covid privacy data available to police" . BBC News, 5 de janeiro de 2021. Disponível em: https://www.bbc.com/news/world-asia-55541001. Acesso em: 26/10/2021.

LEONARDI, Marcel. *Transferência internacional de dados pessoais*. In: *Tratado de proteção de dados Pessoais*. Rio de Janeiro: Forense, 2021.

LISS, Daniel. "*Today's real story: The Facebook monopoly"* in Tech Crunch, 19 de agosto de 2021. Disponível em: https://techcrunch.com/2021/08/19/todays-real-story-the-facebook-monopoly/. Acesso em 28/11/2021.

MASCARENHAS, Fernanda. *O regime de transferência Internacional de dados da LGPD: Delineando as opções regulatórias em jogo*. In: Tratado de proteção de dados Pessoais" Forense: Rio de Janeiro, 2021.

MATHIESEN, Thomas. Towards a Surveillant Society: The Rise of Surveillance Systems in Europe Londres: Waterside Press, 2013.

MUNIZ, Mariana. *A terceira onda de interpretação do Marco Civil no STJ*. In: JOTA, 17 de

Julho de 2017. Disponível em: https://www.jota.info/justica/a-terceira-onda-de-interpretacao-do-marco-civil-no-stj-17072017. Acesso em 28/11/2021.

NICHOLS, Shaun. *ExpressVPN stands behind CIO named in UAE hacking scandal*. In: Tech Target, 16 de setembro de 2021. Disponível em: https://www.techtarget.com/searchsecurity/news/252506801/ExpressVPN-stands-behind-CIO-named-in-UAE-hacking-scandal. Acesso em 28/11/2021.
PASQUALE, Frank. The Black Box Society. *The Secret Algorithms That Control Money and Information.* Londres: Harvard University Press, 2015.

SARLET, Ingo. *Fundamentos Constitucionais: O direito fundamental à proteção de dados*. In: BIONI, Bruno (coordenador Executivo) *Tratado de proteção de dados Pessoais*. Rio de Janeiro: Forense, 2021, Ebook, pos 300;

_____, Ingo. *A eficácia dos direitos fundamentais: Uma teoria geral dos direitos fundamentais na Perspectiva Constitucional*. Porto Alegre: Livraria do Advogado, 12ª edição, 2015.

_____, Ingo. *Proteção de dados pessoais como Direito Fundamental na constituição Federal Brasileira de 1988: Contributo para a construção de uma dogmática constitucionalmente adequada.* Belo Horizonte Revista Direitos Fundamentais e justiça, 2020, ano 14, n 42, p 179-218, jan-jun 2020;

_____, Ingo. *O conceito de direitos fundamentais na Constituição Federal de 1988*. 27 de fevereiro de 2015. Disponível em: https://www.conjur.com.br/2015-fev-27/direitos-fundamentais-conceito-direitos-fundamentais-constituicao-federal-1988. Acesso em: 25/05/2021

SOLOVE, Daniel. *Understanding Privacy.* Londres: Harvard University Press, 2008.

STAR, Leigh. *This is not a boundary object: Reflections on the origin of a concept*. In: Science, Technology, & Human Values, 35(5), 601–617. Disponível em: https://doi.org/10.1177/016224391037762 Acesso em 29/10/2021.

ZUBOFF, Shoshana. *Big Other: capitalismo de vigilância e perspectivas para uma civilização de informação* in*: Tecnopolíticas da vigilância: perspectivas da margem*. Organização: Fernanda Brunoet al.] . Tradução: Heloísa Cardoso Mourão et al1. ed.. São Paulo: Boitempo, 2018.

ZUBOFF, Shoshana. *The age of surveillance capitalism*. Nova York: Public Affairs, 2019.

WIMMER, Miriam. *O regime jurídico do tratamento de dados pessoais pelo Poder público*. In: BIONI, Bruno (coordenador Executivo). *Tratado de proteção de dados Pessoais.* Rio de Janeiro: Forense, 2021.

Recebido em: 30/11/2021
1º Parecer em: 09/02/2022
2º Parecer em: 17/05/2022