



# CYBERVIGILÂNCIA, DADOS E VIOLAÇÕES DE DIREITOS HUMANOS: Debates desde o caso *The Big Brother Watch et al. vs. Reino Unido*

Submetido em: 26-08-2024  
Publicado em: 02-12-2024

**Tatiana Cardoso Squeff**

Doutora em Direito, UFRGS  
✉ [tatiafrcardoso@gmail.com](mailto:tatiafrcardoso@gmail.com)

**Jose Luis Bolzan de Moraes**

Doutor em Direito, UFRGS  
✉ [bolzan@hotmail.com](mailto:bolzan@hotmail.com)

**RESUMO:** A cibernética da vida tem permitido que atos diários ordinários sejam mapeados, coletados, analisados e armazenados em ambiente digital. Diante desse quadro, tem-se que os dados pessoais transformaram-se em verdadeiros ativos na sociedade em rede hodierna, os quais, caso não sejam devidamente manipulados pelo Estado, podem ensejar a violação de direitos humanos. Em vista disso, essa investigação busca expor essa nova cyberrealidade e a importância dos dados, debatendo-se, em seguida, a/o coleta/processamento/uso incorreto de dados pessoais pelo Estado, questionando a existência de requisitos a serem seguidos pelas autoridades nacionais ao fazê-la/o. Para tanto, desde um estudo dedutivo, realiza-se um estudo de caso, explorando-se a recente decisão da Corte Europeia de Direitos Humanos no caso *The Big Brother Watch et al. vs. Reino Unido*. Ademais, frisa-se que os objetivos serão analisados desde os métodos descritivo, explicativo e analítico, sendo desenvolvidos também desde as técnicas bibliográfica e documental de pesquisa, selecionadas qualitativamente desde as palavras-chave deste texto.

**Palavras-chave:** cybervigilância; dados pessoais; quantificação algorítmica; direitos humanos; *The Big Brother Watch et al. vs. Kingdom*.

## CYBER SURVEILLANCE, DATA AND HUMAN RIGHTS VIOLATIONS: Debates arising from *The Big Brother Watch et al. vs. Uk Case*

**ABSTRACT:** *The cybernetization of life has allowed ordinary daily acts to be mapped, collected, analyzed and stored in a digital environment. In view of this, personal data have become true assets in today's network society, which, if not properly handled by the State, can lead to the violation of human rights. Hence, this investigation seeks to expose this new cyberreality and the importance of data, debating, then, the collection/processing/incorrect use of personal data by the State, questioning the existence of requirements to be followed by the domestic authorities when doing so. Therefore, from a deductive method of approach, a case study is carried out, exploring the recent decision of the European Court of Human Rights in the case The Big Brother Watch et al. vs. Kingdom. Furthermore, it is emphasized that the objectives will be analyzed from the descriptive, explanatory and analytical methods, being also developed from the bibliographic and documentary research techniques, qualitatively selected from the keywords of this text.*

**Keywords:** cybersurveillance; personal data; algorithmic quantification; human rights; The Big Brother Watch et al. vs. Kingdom.

## 1 INTRODUÇÃO

Na atualidade, com a crescente digitalização e cibernização da vida, os atos diários mais ordinários podem ser mapeados, coletados, analisados e armazenados em ambiente digital, haja vista a produção de dados provenientes da conexão dos seres humanos e de suas atividades às redes. Nesse passo, antecipar uma compra, uma preferência, um gesto ou mesmo uma necessidade já são ações bastante corriqueiras as quais os indivíduos estão submetidos nessa nova realidade. Isso decorre em grande medida dos avanços obtidos na área da tecnologia da informação, sobretudo, pela atuação de *big techs*, as quais cada vez mais promovem essa informacionalização da vida, transformando, conseqüentemente, os dados pessoais em ativos econômicos importantíssimos para a realização de suas atividades.

Ocorre que a operação de tais empresas não acontece mais em um lugar fixo, como no passado. As *big techs* não só beberam da globalização do mercado proveniente da transnacionalização da divisão internacional do trabalho, como também têm hoje grande parte das suas operações realizadas nas próprias redes, perpassando por diversas jurisdições. No

tocante aos dados produzidos no ambiente informacional, por exemplo, nota-se que a sua captação e transferência podem se dar em uma localidade, enquanto o seu armazenamento e mineração em outra; e, ainda, uma vez extraídos, eles podem ser usados para finalidades múltiplas (sejam elas positivas ou negativas) e por sujeitos diversos (públicos ou privados), não necessariamente encontrando balizas na legislação de todos os lugares envolvidos, logo, “*defy[ing] international law’s traditional state-centric paradigm*” (PETERS, 2017, p. 151).

A interceptação, coleta, análise e arquivamento de dados, portanto, são um exemplo bastante significativo desse novo mundo que se inaugura com a Sociedade em Rede, introduzindo diversas dificuldades para o Direito hoje aplicável. Afinal, a depender do que se faz com tais dados, eles podem causar impactos significativos para a proteção dos direitos humanos, como o direito à privacidade ou mesmo o direito de liberdade de expressão, para citar alguns, tal como assentou a própria Assembléia Geral das Nações Unidas ainda em 2014 quando debatendo o crescimento da vigilância e monitoramento pessoal na Era Digital (UNITED NATIONS, 2014, preâmbulo).

De se recordar que essa foi a mesma época em que o escândalo da *National Security Agency* veio à tona a partir das denúncias realizadas por Edward Snowden, sobre a coleta de dados e o monitoramento realizado em larga escala por parte deste país a indivíduos situados naquele Estado e no exterior, materializando, assim, o aspecto negativo da digitalização da vida. Pior ainda, pois, realizado não apenas pelo Estado, que, em teoria, deteria o dever primário de zelar pelos direitos humanos, como também foi um ato replicado em outras regiões, como, por exemplo, no Reino Unido. Outrossim, argumentam essas nações que tais condutas estariam autorizadas pelas próprias regras de direitos humanos, as quais não seriam absolutas, muito embora existam posicionamentos contrários<sup>165</sup>.

Diante desse quadro, considerando que os direitos humanos seriam uma baliza natural para uma atuação irrestrita do Estado (e também para aqueles que operariam dentro deste em virtude da horizontalidade destes direitos) no que tange à coleta e ao processamento de dados pessoais, questiona-se justamente se existiram outros requisitos a serem observados para evitar abusos, ou se realmente o Direito restou atrás do seu tempo, para dialogar com Ost (1999), exigindo-se a sua imediata renovação. Para tanto, utilizando-se do repertório de jurisprudência publicado pela Corte Europeia de Direitos Humanos – CEDH – em março de 2022 sobre os principais casos julgados no ano anterior (CEDH, 2021), selecionou-se o caso

---

<sup>165</sup> Como relata Peters (2017, p. 149), “*The U.N. High Commissioner’s report on Privacy in the Digital Age even held that [t]he very existence of a mass surveillance programme [...] creates an interference with privacy*”.

*The Big Brother Watch et al. vs. Reino Unido* como ponto de diálogo, justamente porque ele aborda a cybervigilância e o uso de dados individuais por parte do Estado.

Por fim, no que tange os aspectos metodológicos, esta investigação será realizada a partir da abordagem dedutiva, em que, em um primeiro momento busca-se compreender os aspectos centrais da Sociedade em Rede e a relevância que a coleta, processamento e manipulação de dados vem adquirindo, para que, posteriormente, possa-se adentrar no estudo do julgado da CEDH de maneira pormenorizada, buscando responder a pergunta que dirige este estudo, ou seja, se existem requisitos adicionais quando da coleta, análise, arquivamento e transferência de dados pessoais. Assim sendo, tem-se que objetivos serão analisados desde os métodos descritivo, explicativo e analítico, sendo desenvolvidos desde as técnicas de estudo de caso, utilizando-se do citado precedente do tribunal europeu, além das técnicas bibliográfica e documental de pesquisa, selecionadas qualitativamente desde as palavras-chave deste texto.

## **2 DA SOCIEDADE EM REDE À QUANTIFICAÇÃO ALGORÍTMICA: A RELEVÂNCIA E O USO DE DADOS NA ATUALIDADE**

Os desenvolvimentos tecnológicos hoje existentes, sem dúvidas, promoveram mudanças significativas na sociedade. Não só em termos econômicos, militares e de bem-estar, saúde e lazer (CASTELLS, 1999, p. 44), mas, sobretudo, na experiência social como um todo, isto é, na “vivência do espaço e do tempo”, notadamente com o advento e propagação da internet e da sociedade em rede (CARDOSO, 1999, p. 37). Afinal, tanto o espaço quanto o tempo se flexibilizam nas relações havidas de forma *online*. Não há mais que se falar em fronteiras territoriais rígidas nas redes, e a instantaneidade é uma marca dessa nova realidade.

Segundo Castells (1999, p. 51), a dinâmica social introduzida pelo crescente informacionalismo (também chamado por ele de pós-industrialismo<sup>166</sup>), estaria associada ao surgimento de novos meios de produção, experiência e poder. De fato, considerando a

---

<sup>166</sup> Explica Castells (1999, p. 54) que “o industrialismo é voltado para o crescimento da economia, isto é, para a maximização da produção; o informacionalismo visa o desenvolvimento tecnológico, ou seja, a acumulação de conhecimentos e maiores níveis de complexidade do processamento da informação. Embora graus mais altos de conhecimentos geralmente possam resultar em melhores níveis de produção por unidade de insumos, é a busca por conhecimentos e informação que caracteriza a função da produção tecnológica no informacionalismo”, sendo essa, portanto, a distinção crucial entre o período industrialista e o pós-industrialista.

‘produção’ “a ação da humanidade sobre a matéria para apropriar-se dela e transformá-la em seu benefício” (CASTELLS, 1999, p. 51), tem-se que, hodiernamente, os dados são uma espécie de nova matéria-prima<sup>167</sup>. Deles é possível não apenas obter e aprimorar produtos, como também guiar o consumo humano e os investimentos. Inclusive, como destacou a *The Economist*, os dados seriam o novo petróleo dada a sua influência e relevância na atual sociedade.<sup>168</sup>

No que tange a ‘experiência,’ sendo esta a “ação dos sujeitos humanos sobre si mesmos, determinada pela interação entre as identidades biológicas e culturais desses sujeitos em relação a seus ambientes sociais e naturais” (CASTELLS, 1999, p. 51), quase todos os atos da vida humana estão informatizados e, logo, de alguma forma conectados às redes. Isso porque, “*whether you are going for a run, watching TV or even just sitting in traffic, virtually every activity creates a digital trace*” na sociedade da informação (THE ECONOMIST, 2017).

Quanto ao ‘poder’, na medida em que este se refere à “relação entre os sujeitos humanos que, com base na produção e na experiência, impõe a vontade de alguns sobre outros pelo emprego potencial ou real de violência física ou simbólica” (CASTELLS, 1999, p. 51), mostra-se igualmente notório como o uso dos dados pode terminar por induzir o comportamento humano. Por certo que não pelo uso de força física, mas sim por meio da persuasão, que, pelo advento da internet das coisas<sup>169</sup>, podem conduzir o indivíduo ao consumo de certo produto ou serviço. Isso, pois, o processamento de dados obtidos através da

---

<sup>167</sup> “*Capitalism has turned to data as one way to maintain economic growth and vitality in the face of a sluggish production sector. In the twenty-first century, on the basis of changes in digital technologies, data have become increasingly central to firms and their relations with workers, customers, and other capitalists*” (SRNICEK, 2017, p. 10).

<sup>168</sup> “*A new commodity spawns a lucrative, fast-growing industry, prompting antitrust regulators to step in to restrain those who control its flow. A century ago, the resource in question was oil. Now similar concerns are being raised by the giants that deal in data, the oil of the digital era*” (THE ECONOMIST, 2017).

<sup>169</sup> Segundo Riemenschneider e Mucelin (2021, p. 692), “a expressão Internet das Coisas (IdC) tem sua origem na língua inglesa, *Internet of Things*, e apareceu pela primeira vez em 1995 nas produções de Kevin Ashton, cofundador do *MIT Auto ID Center*. [...] [D]entre as diversas interpretações possíveis, pode-se, de maneira geral, estabelecer que se trata da conexão de objetos físicos à Internet, entre si e com o usuário, por meio de sensores e tecnologias *wireless*, tornando-os capazes de interagir com ambiente e com as pessoas, com capacidade de responsividade em tempo real”; ou seja, trata-se de “um ecossistema tecnológico próprio, o qual transmite e recebe informações” em rede.

digitalização da vida<sup>170</sup> feito por “*algorithms can predict when a customer is ready to buy, a jet-engine needs servicing or a person is at risk of a disease*” (THE ECONOMIST, 2017).

Assim, tem-se que a informação correntemente passada por meio da geração e do processamento de dados é o motor central da sociedade em rede, vez que esta é a fonte da produtividade, a qual acaba determinando a própria experiência humana na medida em que impacta a forma do ser em relacionar-se com o meio e de comunicar-se com os demais, e refunda o poder, posto que o Estado acaba perdendo o monopólio que antes detinha da ‘violência’ (aqui interpretada como controle social), compartilhando-a com as titãs da tecnologia da informação como *Alphabet (Google), Amazon, Apple, Facebook e Microsoft*.

Trata-se, portanto, de um novo paradigma – um “paradigma tecnológico baseado na tecnologia da informação” que está em constante aprimoramento.<sup>171</sup> Afinal, já existe um “complexo de tecnologias” na segunda década do século XXI que vão muito além da mera conversão da tecnologia analógica, a qual já conectava as pessoas em diferentes escalas no passado, em digital. Para além das já citadas internet das coisas e da *big data analytics*, destaque-se, ainda, a própria Internet 5G e versões posteriores, *cloud computing*, Inteligência Artificial, *Blockchain* e *computing power*, “que, reunidas, dão azo ao ambiente propício para a formação de um ecossistema tecnológico que promete a melhoria das condições de vida e de eficiência econômica” (SQUEFF, MUCELIN, 2021, p. 447).

Um ecossistema, entretanto, que pode ser considerado igualmente invasivo no que toca a esfera da privacidade dos cidadãos e outras liberdades clássicas, como de escolha e expressão. Os efeitos de se estar em rede, particularmente quanto “ao uso intensivo de dados e sistemas de análise e estruturação desses dados (via *machine learning* e *deep learning*, por exemplo)” (SQUEFF, MUCELIN, 2021, p. 447), todavia, permitem que o “*Google see what*

---

<sup>170</sup> Pode-se entender essa digitalização da vida como um aspecto da própria transformação digital a qual o mundo perpassa, “como a construção de representações do mundo físico no mundo virtual (*digitaler Zwilling*), as quais estão em contínuo aperfeiçoamento, cujas características são a inevitabilidade, a irreversibilidade, a rapidez e a incerteza quanto aos seus detalhes”. A digitalização, especificamente, pode ser “caracterizada pela adoção em larga escala de tecnologias [...], o qual fagocita as dinâmicas sociais e econômicas e que, portanto, influenciam todos os aspectos da vivência humana” (SQUEFF, MUCELIN, 2021, p. 447).

<sup>171</sup> Sobre o tema trouxe Castells, visionariamente, na década de 1990: “[...] conhecimento e informação são elementos cruciais em todos os modos de desenvolvimento, visto que o processo produtivo sempre se baseia em algum grau de conhecimento e no processamento da informação. Contudo, o que é específico ao modo informacional de desenvolvimento é a ação de conhecimento sobre os próprios conhecimentos como principal fonte de produtividade. O processamento da informação [logo, incluindo-se de dados] é focalizado na melhoria da tecnologia do processamento da informação como fonte de produtividade, em um círculo virtuoso de interação entre as fontes de conhecimentos tecnológicos e a aplicação da tecnologia para melhorar a geração de conhecimento e o processamento da informação: é por isso que, voltando à moda popular, chamo esse novo modo de desenvolvimento de informacional, constituído pelo surgimento de um novo paradigma tecnológico baseado na tecnologia da informação” (CASTELLS, 1999, p. 53-54).

*people search for, Facebook what they share, Amazon what they buy*” (THE ECONOMIST, 2017). Dito de outro modo, *“today, metadata could print a detailed and intimate picture of a person: they allowed for mapping of communication patterns, and insight into who a person interacted with”* (CEDH, 2021). E os Estados, cientes disso, igualmente passaram a utilizar-se dos dados para exercer a vigilância sob os indivíduos territorial e extraterritorialmente.

Veja-se o caso da *National Security Agency* (NSA, na sigla em inglês) estadunidense, exteriorizado por Edward Snowden, em 2013, de que o governo dos Estados Unidos se utilizava da obtenção e análise de dados pessoais por meio da vigilância de indivíduos *online* na tentativa de angariar informações teoricamente voltadas ao combate ao terrorismo, inclusive, sem a necessidade de mandados judiciais (BALKIN, 2008, p. 1-2). Outrossim, tal programa, como demonstraram os arquivos repassados por Snowden ao jornal *The Guardian*, não se limitavam a pessoas pré-selecionadas pelo seu histórico de envolvimento com causas terroristas, senão a quaisquer indivíduos, estivessem eles fisicamente no país ou não (MACASKILL; BORGER; GREENWALD, 2013), incluindo Chefes de Estado e de Governo (BALL, 2013), como Angela Merkel<sup>172</sup> e Dilma Rousseff<sup>173</sup>.

Outra situação emblemática envolvendo o uso dos dados na atual sociedade informacional se refere à vigilância governamental da própria mídia. Veja-se as recentes acusações de utilização do *Pegasus Spyware* por parte do governo de Viktor Orbán, da Hungria, contra jornalistas independentes, que *“enables the attacker to view all content on a phone, including messages from apps with end-to-end encryption, photographs and GPS location data. It can also turn the device into an audio or video recorder”* (WALKER, 2021). O mesmo *spyware*, produzido em Israel e vendido exclusivamente para governos, também teve seu uso denunciado em outros países<sup>174</sup>, como em El Salvador, em 2022, por parte do Presidente Nayib Bukele contra jornalistas investigativos (LINTHICUM, 2022). Outros

---

<sup>172</sup> Sobre o impacto da vigilância sob Angela Merkel e a repercussão na Alemanha, inclusive, no que toca a participação de instituições domésticas alemãs no esquema, cf. SHULZE, 2015.

<sup>173</sup> A Ex-Presidenta Dilma não foi a única autoridade brasileira sujeita à vigilância estadunidense. Nelson Barbosa, que foi secretário executivo do Ministério da Fazenda, José Elito Carvalho Siqueira, que à época foi chefe do Gabinete de Segurança Institucional, Antonio Palocci, ex-chefe da Casa Civil, Luiz Awazu Pereira da Silva, ex-diretor do Banco Central, e o ex-ministro das Relações Exteriores do Brasil Luiz Alberto Figueiredo também tiveram seus telefones grampeados. A mídia reporta que o caso foi deixado de lado em função da crise econômica que o país perpassava, não havendo repercussões maiores, como na Alemanha. Cf. WIKILEAKS, 2015; SCHOSSLER, 2015.

<sup>174</sup> Consoante a *Amnesty International*, além de El Salvador e Hungria, outros 10 países igualmente o estariam utilizando, a saber: Arábia Saudita, Azerbaijão, Bahrein, Emirados Árabes Unidos, Índia, Cazaquistão, México, Marrocos, Ruanda e Togo. Cf. AMNESTY INTERNATIONAL, 2021.

*spywares* semelhantes, como o *Predator*, também tem tido o seu uso contra jornalistas denunciado na Grécia (GIUSSANI, 2022).

Ademais, o uso de *fake news* também é bastante emblemático, pois, espalhadas a partir das preferências algorítmicas dos usuários da internet que são determinadas por meio da coleta de dados de plataformas por eles usadas, como o *Facebook*, denotam as intrínsecas imbricações entre o setor público e o privado no ambiente em rede. Na medida em que objetiva “desestabilizar o conhecimento, desestruturar as pessoas incutindo medo e dúvida que alimentam a desinformação”, a disseminação de *fake news* a pessoas algoritmicamente escolhidas culmina na persuasão, inibição ou desestímulo de uma determinada ação (LOBO; MORAIS; NEMER, 2020), implicando diretamente na liberdade de escolha, como, por exemplo, o voto em determinado candidato (como ocorrera na corrida presidencial estadunidense de 2016, por parte de Donald Trump<sup>175</sup>, e no pleito brasileiro de 2018, por parte de Jair Bolsonaro<sup>176</sup>) ou o questionamento de certa ação governamental (como no caso da pandemia de Covid-19 no Brasil, no que se refere ao uso retórico-falseado sobre o número de casos e de óbitos, e medidas de prevenção e de tratamento<sup>177</sup>).

Aliás, *fake news*, quando disparadas por meio das redes, utilizando-se de plataformas como *Twitter*, *Facebook* e *YouTube*, também são exemplos de como a (re)produção algorítmica de dados igualmente podem gerar impactos no que tange o direito intrínseco das pessoas de receberem informação correta – um eixo do direito da liberdade de expressão. Afinal, por meio da “desintermediação”, isto é, por meio de canais de interlocução direta com o público em geral (PEREIRA, 2021, p. 100), as quais apresentam “maior poder que rádio ou TV” (LOBO; MORAIS, 2019, p. 1081), a sociedade pode acabar recebendo informações

<sup>175</sup> Aqui refere-se ao uso da *Cambridge Analytica* que vendera dados de cerca de 50 milhões de perfis de estadunidenses aptos a votar, obtidos junto ao *Facebook*, coletados por meio do aplicativo *this is your digital life*, para a sua campanha presidencial, para fins de manipulação eventual por meio de *fake news* (MARTINS; TATEOKI, 2019). Cf, também: BOVET; MAKSE, 2019.

<sup>176</sup> Aqui, refere-se ao uso de milícias digitais, as quais “atuaram fortemente nas eleições de 2018, oportunidade em que preferiram o uso das redes privadas do *WhatsApp*, aplicativo de fácil utilização, que difunde de modo muito rápido as mensagens segredadas pela criptografia, que só permite ao destinatário desembaralhá-las e replicá-las, numa rede interminável que se mostrou de extrema eficiência”. Afinal, mesmo que existam “47 milhões de brasileiros que não usam a internet as, claro, os que têm celular, na sua maioria arrasadora, adotam esse aplicativo como meio de comunicação pela troca de mensagens e (des)informações, daí a razão de ter atraído a atenção das milícias digitais, porque acessível, popular e sem controle externo” (LOBO; MORAIS; NEMER, 2020, p. 264-265).

<sup>177</sup> “Foram identificadas 329 *fake news* relacionadas à pandemia de COVID-19 nos sites estudados (253 no G1 e 76 no Ministério da Saúde). As *fake news* foram disseminadas principalmente através de *WhatsApp* e *Facebook*. As categorias temáticas mais frequentes foram: política (por exemplo, governantes falsificando a vacinação contra a COVID-19, com 20,1%), epidemiologia e estatística (proporção dos casos e óbitos, 19,5%) e prevenção (16,1%). Conforme o *Google Trends*, houve um aumento de 34,3% nas buscas que utilizavam termos presentes nas *fake news*” (BARCELOS, 2021).



inverídicas e cujas fontes não são confiáveis – o que a mídia tradicional, por exemplo, tem o dever de verificar, zelando pelo interesse público.

Não é por outra razão que Levitsky e Ziblatt (2018, p. 71 e 169) apontaram o enfraquecimento da mídia tradicional como sendo um atentado à própria democracia, citando exemplos de Trump, nos Estados Unidos, Fujimori, no Peru, Chávez, na Venezuela, e Erdogan, na Turquia. Mas certamente não se pode deixar de fora os episódios envolvendo o Brasil corrente e o uso das redes por Jair Bolsonaro, em que o mesmo acaba disseminando *fake news* por meio de seus *tweets* e *lives* (PEREIRA, 2021, p. 102-104), por vezes, inclusive, atacando diretamente a imprensa tradicional<sup>178</sup> e, logo, a sua legitimidade e o seu importante papel de guardião do interesse da sociedade como um todo, dando ensejo a discussões que vão desde a responsabilidade individual deste<sup>179</sup>, do Estado ou mesmo das próprias redes<sup>180</sup>, seja de maneira singular<sup>181</sup> ou compartilhada<sup>182</sup>, pela amplificação gerada às *fake News* (MENEZES, 2020, p. 163) e os consequentes ataques aos direitos humanos (LOBO; MORAIS; NEMER, 2020, p. 257).

De qualquer forma, o que se verifica é que, ao lado das gigantes tecnológicas, os Estados também usam dos avanços informacionais e quantitativos<sup>183</sup> para a realização de suas atividades, sobretudo, por meio da vigilância e direcionamento, “infiltrando-se e se

---

<sup>178</sup> Segundo a organização 'Repórteres Sem Fronteira', por exemplo, Bolsonaro foi responsável a 88% de ataques a imprensa tradicional no primeiro semestre de 2021. Pessoalmente, ele atacou a imprensa em 87 ocasiões no 1º semestre de 2021, correspondendo a um aumento de 74% em relação ao 2º semestre de 2020 (PODER 360, 2021).

<sup>179</sup> Sobre o tema, importante destacar os debates envolvendo a Lei Federal brasileira de n. 14.197 de 2021, mais conhecida como a "nova lei de segurança nacional". Isso porque, o Presidente Jair Bolsonaro, quando da sanção da mesma, vetou explicitamente a tipificação do 'crime de comunicação enganosa em massa', o qual atribuía uma pena de até cinco anos de reclusão para quem o cometesse, sob o argumento de que isso violaria a 'liberdade de expressão'. Salienta-se que o veto presidencial pode ser derrubado pelo Congresso, porém, até maio de 2022, o tema ainda não foi pautado. Cf. AGÊNCIA SENADO, 2021; AGÊNCIA CÂMARA, 2022.

<sup>180</sup> “*The spread of false, manipulated or out-of-context information as a standard of intervention [...] raises the question of the abuse of mass media in its virtual form, inviting us to reflect on the liability, also, of the companies that supply this technology, in order to protect political guarantees and human rights*” (LÓBO; MORAIS, 2019, p. 1079). No Brasil, o “debate legislativo sobre regulação das redes sociais no combate às *fake news* gira em torno de [...] propostas que atribuem responsabilidade [das redes] perante terceiros por danos causados pela desinformação veiculada, caso os provedores de aplicação não retirem do ar, no prazo estipulado, o conteúdo reclamado” (MARANHÃO; ABRUSIO; CAMPOS, 2020).

<sup>181</sup> “[...] a responsabilização de quem financia o crime organizado nas redes, inclusive e principalmente, pessoas jurídicas e agentes estatais” (LOBO; MORAIS; NEMER, 2020, p. 269).

<sup>182</sup> “Profissionais e pesquisadores de redes sociais, imprensa e direito defenderam, na Câmara dos Deputados, a responsabilidade compartilhada de Estado, plataformas digitais e usuários no combate à difusão de notícias falsas” (AGÊNCIA CÂMARA, 2021).

<sup>183</sup> Lobo, Morais e Nemer (2020, p. 256) explicam que, com o “[...] avanço da internet, do desenvolvimento de algoritmos, da inteligência artificial e, mais recentemente, da internet das coisas, além de outras constantes mudanças tecnológicas, passamos da era da informação para a da quantificação, como sugerido por Éric Sadin”, em que os processos numéricos e matemáticos – algorítmicos – ganham cada vez mais espaço (grifo não constante no original).

espalhando em muitas áreas da vida sobre as quais sua influência era apenas marginal” (BAUMAN, 2013, p. 7). E, assim, confirma-se a existência, na atualidade, de um verdadeiro Estado de vigilância – “*a state that tries to identify and solve problems of governance through the collection, collation, analysis, and production of information*” (BALKIN, 2008, p. 3). Mais especificamente, neste Estado, segundo Balkin (2008, p. 3), entidades públicas e privadas usam “*surveillance, data collection, collation, and analysis to identify problems, to head off potential threats, to [selectively and effectively]<sup>184</sup> govern populations, and [sometimes] to deliver valuable social services*”, exercendo um controle similar àquele concebido na famosa distopia Orwelliana, ‘1984’<sup>185</sup>.

Contudo, nessa *cybervigilância* hodierna, para dialogar tanto com Bauman como Lévy (1999)<sup>186</sup>, o problema que emerge é justamente o *poder* que tal monitoramento “exercido por departamentos governamentais, agências de polícia e corporações privadas” pressupõe, posto que ele “agora existe num espaço global e extraterritorial”, que eventualmente foge de eventuais amarras antes introduzidas pelos Estados localmente, por meio de políticas ou normas domésticas (BAUMAN, 2013, p. 7), culminando, por vezes, na violação de direitos humanos, como, exemplificativamente, tal como avultado *supra*, o direito à vida privada e a liberdade de expressão (aqui, compreendida como ter acesso a informação

---

<sup>184</sup> Aqui, adicionam-se esses advérbios em alusão à expressão cunhada por Pariser de ‘*bubble democracy*’, que seria “um estado de isolamento intelectual que pode resultar de pesquisas personalizadas *online* quando um algoritmo [através dos dados disponibilizados à plataforma acessada] adivinha seletivamente quais informações um usuário gostaria de ver com base em informações sobre ele, como localização, comportamento de cliques e histórico de pesquisas. Como resultado, os usuários ficam separados de informações que não concordam com seus pontos de vista, isolando-os efetivamente em suas próprias bolhas culturais ou ideológica” (grifo não constante no original) (PARISER, 2011, *apud* LOBO; MORAIS; NEMER, 2020, p. 258).

<sup>185</sup> Orwell restou conhecido por sua obra 1984, justamente ao pensar em um futuro distópico um tanto perturbador em que o Estado, o grande Irmão, estaria sempre vigiando e direcionando o cidadão, limitando a sua capacidade racional individualizada e a existência de contrapontos, por meio de mecanismos opressivos, excludentes e institucionalizados. O Estado, nesse ambiente, seria onipresente, detentor da verdade e logo, controlador da sociedade. Orwell não faz alusão a entidades privadas, em que pese os ‘dois minutos de ódio’ relatados no livro como forma de agressão simbólica ao outro, se assemelham a situações hoje experimentadas no *Facebook, Instagram, Twitter, Youtube e WhatsApp*. Cf. ORWELL, 2009.

<sup>186</sup> Lévy, ao denotar a formação e a existência de uma cultura informática coletiva, composta por “técnicas (materiais e intelectuais), de práticas, de atitudes, de modos de pensamento e de valores que se desenvolvem juntamente com o crescimento do ciberespaço” nos dias atuais, denominou-a de cibercultura – uma nova configuração social levada a cabo por sistemas de circulação e processamento de informação disponíveis *online*, que media as relações dos seres humanos com o universo. Este, pontualmente, chamado de ciberespaço, que interconecta mundialmente os indivíduos, não se refere “apenas a infraestrutura material da comunicação digital, mas também o universo oceânico de informações que ela abriga, assim como os seres humanos que navegam e alimentam esse universo” (LEVY, 1999, p. 17). Nesse passo, dentro da cibercultura é que se aduz brotar a *cybervigilância*, vez que os indivíduos são submetidos a sistemas de “monitoramento, controle, observação, classificação, checagem e atenção sistemática” neste universo (BAUMAN, 2013, p. 3).

de interesse público), os quais merecem a devida atenção e repercussão notadamente em virtude do retrocesso que ela pode ensejar dentro de uma democracia<sup>187</sup>.

E exatamente sobre este tema é que ganha importância debater o caso *The Big Brother Watch vs. Reino Unido*, julgado pela Corte Europeia de Direitos Humanos em 2021, envolvendo o uso incorreto de dados pessoais no contexto da cybervigilância estatal, na medida em que ele oferece parâmetros a serem seguidos pelos Estados quando desejando coletar e fazer uso de tais dados, acerca do qual se debruçará no ponto subsequente.

### 3 LIMITES À CYBERVIGILÂNCIA? REFLEXÕES DESDE O CASO ‘THE BIG BROTHER WATCH VS. REINO UNIDO’

O caso *The Big Brother Watch vs. Reino Unido*, julgado pela CEDH em 2021, tem como base três *applications* trazidas contra o Reino Unido entre os anos de 2013 e 2015, tendo como objetivo questionar “*the scope and magnitude of the electronic surveillance programmes operated by the Government of the United Kingdom*” (CEDH, 2021, para. 3). Mais especificamente, as demandas questionavam as condutas do serviço de inteligência britânico (o *Government Communications Headquarters* – GCHQ, na sigla em inglês) no âmbito da operação chamada ‘Tempora’, a qual interceptava e grampeava as comunicações de diversas pessoas situadas no exterior (mas que, claro, tivessem alguma relação com o Reino Unido<sup>188</sup>), como também armazenava dados das mesmas para fins de eventual análise em investigações (CEDH, 2021, para. 15).

Apesar de ser previsto em lei, mais especificamente no *Regulation of Investigatory Powers Act* (2000), os dados – que não necessariamente precisariam estar em domínio público, notadamente em casos envolvendo a segurança nacional – eram angariados a partir de critérios bastante simplificados e genéricos, de modo que “*any communication which matched the simple selectors were collected*” (CEDH, 2021, para. 17 e 38). Inclusive,

---

<sup>187</sup> Lobo, Morais e Nemer (2020, p. 258) tecem uma dura crítica a democracia hodierna, pois, “turbinada por algoritmos e *fake news*, libertou um sistema de correntes de opinião que ‘se movem em enxames de trajetórias imprevisíveis e cambiantes, alimentados, principalmente, por uma carga de ressentimento’, afetando os instrumentos de eleição e de decisão, as próprias estratégias políticas dos procedimentos decisórios, além de instaurar um ambiente de ódio e rejeição, incompatível com o caráter incluyente e de aceitação das diferenças, peculiares ao jogo democrático”. Inclusive, dão a ela o nome de *fake democracy*.

<sup>188</sup> Importante dizer que as comunicações passíveis de interceptação e de retenção de dados pela GCHQ não poderiam estar total e exclusivamente no Reino Unido. Outrossim, se armazenadas no exterior, como nos Estados Unidos, poderiam ser objeto de ação (a não ser que envolvesse cidadão americano). Cf. CEDH, 2021, para. 74-75.

quaisquer comunicações relacionadas àquelas de interesse (seja relativa ao autor, seja relativa ao destinatário intencional ou eventual) poderiam ser objeto de captação (CEDH, 2021, para. 71). Até mesmo comunicações de jornalistas (CEDH, 2021, para. 448).

Para tanto, não era necessária uma autorização judicial prévia, bastando uma breve e genérica autorização (“*warrant*”) proveniente do Executivo (mesmo *branch* ao qual a GCHQ estaria vinculada).<sup>189</sup> Ademais, uma vez retidos, tais dados passavam por um novo processamento algorítmico, o qual selecionava o material de eventual interesse, criando um índice automático que poderia ser, então, verificado e compartilhado por um analista específico (e autorizado) da GCHQ (CEDH, 2021, para. 18, 30 e 96 – p. 24). No que tange ao armazenamento, o material coletado seria mantido em sistema por até cinco anos, diferentemente do previsto em lei local<sup>190</sup>, de modo que, somente então, seriam passíveis de descarte (CEDH, 2021, para. 59).

Além disso, dados em bloco (“*bulk data*”) poderiam ser tanto compartilhados como adquiridos junto a serviços de inteligência estrangeiros, tal como a NSA (agência estadunidense que restou conhecida pelo caso de Snowden, citado anteriormente), o que, de fato, ocorria desde 2010, pois previsto no acordo entre os Estados, assim como assinalado no *Counter-Terrorism Act* de 2008 (CEDH, 2021, para. 21-22, 24-25, 96 – p. 34, 111, 117 e 140-141). Em que pese nesse caso *data mining* não fosse possível, ainda assim acessavam-se dados específicos de quaisquer pessoas situadas fora do Reino Unido (exceto de cidadãs americanas, em virtude de acordo celebrado entre os países) quando utilizando buscas simplificadas de palavras-chave, catalogadas automaticamente pelo sistema britânico (CEDH, 2021, para. 23 e 25).

Nesse passo, questionavam os autores se a obtenção por parte da GCHQ de *bulk data* de diversos indivíduos, o seu processamento e análise, além da sua própria retenção e compartilhamento com os Estados Unidos, seria legítima à luz dos artigos 8 e 10 da Convenção Europeia de Direitos Humanos (CEDH, 2021, para. 30). Enquanto o artigo 8 prevê o ‘direito ao respeito pela vida privada e familiar’, o artigo 10 contempla a ‘liberdade de expressão’, os quais são assim prescritos:

---

<sup>189</sup> Ressalta-se que os critérios que seriam analisados “*were expressed in very general terms*” em tais mandatos autorizados pelo Ministro/Comissário. Cf. CEDH, 2021, para. 50, 88 e 146.

<sup>190</sup> O *Regulation of Investigatory Powers Act* prevê, no artigo 16(3A), que nos casos de Segurança Nacional a retenção máxima de dados seria de seis meses, enquanto que para as demais infrações penais (as quais, porém, deveriam ser considerados ‘crimes graves’), restariam armazenadas por no máximo três meses, ambas passíveis de renovação pelo Secretário de Estado. Cf. CEDH, 2021, para. 87e 96 (p. 25).

## Artigo 8 - Direito ao respeito pela vida privada e familiar

1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.
2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar econômico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros. (grifos não constantes no original)

## Artigo 10 - Liberdade de expressão

1. Qualquer pessoa tem direito à liberdade de expressão. Este direito compreende a liberdade de opinião e a liberdade de receber ou de transmitir informações ou ideias sem que possa haver ingerência de quaisquer autoridades públicas e sem considerações de fronteiras. O presente artigo não impede que os Estados submetam as empresas de radiodifusão, de cinematografia ou de televisão a um regime de autorização prévia.
2. O exercício desta liberdade, porquanto implica deveres e responsabilidades, pode ser submetido a certas formalidades, condições, restrições ou sanções, previstas pela lei, que constituam providências necessárias, numa sociedade democrática, para a segurança nacional, a integridade territorial ou a segurança pública, a defesa da ordem e a prevenção do crime, a proteção da saúde ou da moral, a proteção da honra ou dos direitos de outrem, para impedir a divulgação de informações confidenciais, ou para garantir a autoridade e a imparcialidade do poder judicial. (grifos não constantes no original) (COUNCIL OF EUROPE, 1950).

Acerca dessas regras, cumpre ressaltar que nenhuma delas seria absoluta. Como se percebe da redação dos respectivos preceitos legais, ambas preveem exceções para o pleno gozo de tais direitos. No caso, portanto, discutiu-se se essas exceções estariam presentes, de modo a verificar se cybervigilância conduzida pelos britânicos eventualmente justificar-se-iam.

A primeira questão é a positivação da exceção. Isso, pois, a lei doméstica deve prever com clareza as circunstâncias em que as violações à proteção de dados serão permitidas, fazendo-se “*accessible to the person concerned and foreseeable as to its effects*”<sup>191</sup>. Tal previsão serve para que restem asseguradas a segurança e a ordem pública, além da própria proteção da coletividade, em uma sociedade democrática. No ponto, portanto, referindo-se a outros casos julgados por ela<sup>192</sup>, a Corte determinou (CEDH, 2021, para 335) que as leis

<sup>191</sup> Salienta-se, por oportuno, que “*‘foreseeability’ cannot mean that individuals should be able to foresee when the authorities are likely to resort to such measures so that they can adapt their conduct accordingly. [...] The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures*”, sabendo-se, assim, os eventuais impactos de tais operações, de modo a “*give the individual adequate protection against arbitrary interference*” (CEDH, 2021, para. 332-333).

<sup>192</sup> São os demais julgados (em que pese, registre-se, muitos grande parte trate de interceptação de comunicações): *Affaire Huvig v. France*. (CEDH, 1990, para. 34); *Case of Kruslin v. France* (CEDH, 1990, para 35); *Affaire Valenzuela Contreras v. Spain* (CEDH, 1998, para. 46); *Gabriele Weber and Cesar Richard Saravia*

nacionais deveriam apresentar seis requisitos mínimos para não serem consideradas abusivas no tocante à interceptação, coleta, análise e arquivamento de dados, inclusive, em casos envolvendo a segurança nacional:

*(i) the nature of offences which may give rise to an interception order; (ii) a definition of the categories of people liable to have their communications intercepted; (iii) a limit on the duration of interception; (iv) the procedure to be followed for examining, using and storing the data obtained; (v) the precautions to be taken when communicating the data to other parties; and (vi) the circumstances in which intercepted data may or must be erased or destroyed.* (CEDH, 2021, para 335)

Com isso, se a legislação do país não contiver qualquer um desses itens, a violação da proteção de dados seria ilegal, transgredindo-se consequentemente tanto o artigo 8 quanto o próprio artigo 10, a depender da situação concreta, como em casos envolvendo jornalistas e suas fontes. Ademais, advertiu que, além desses requisitos previstos em lei, outras condições de “*safeguard are therefore pivotal*” quando se trata de operações no ambiente digital (CEDH, 2021, para 332), devendo-se, por isso, fazer-se presentes. São elas: a necessidade, a proporcionalidade e a existência de mecanismos de supervisão.

A necessidade está atrelada a uma intervenção estatal quando envolvendo matéria de segurança pública, para a prevenção ou detecção de um crime grave, e/ou para resguardar o bem-estar econômico do país na medida em que relacionado a atos voltados à garantia da segurança nacional, a qual deve ser compreendida “*in the traditional sense of protecting national sovereignty against internal or external threats*” (CEDH, 2021, para. 96 – p. 24 – e 191 – p. 60-62). Logo, a vigilância por meio de acesso a dados pessoas seria autorizada em casos de atividades “*which threatened the safety or well-being of the State and activities which were intended to undermine or overthrow parliamentary democracy by political, industrial or violent means*” (CEDH, 2021, para. 369); ou mesmo em casos de crimes graves, nos termos da legislação local<sup>193</sup>.

Acerca disso, a Corte reconheceu que os Estados poderiam valer-se da margem de apreciação nacional para apontar se uma determinada violação à proteção de dados seria a

---

v. *Germany* (CEDH, 2006, para 95); *Association for European Integration and Human Rights and Ekimdzhev v. Bulgaria* (CEDH, 2007, para 76); e *Roman Zakharov v. Russia* (CEDH, 2015, para. 231).

<sup>193</sup> Consoante o *Regulation of Investigatory Powers Act* britânico, artigo 81(2)(b), um crime grave seria aquele que “*the perpetrator (assuming he or she was over the age of twenty-one and had no previous convictions) could reasonably be expected to be sentenced to imprisonment for a term of three years or more; or where the conduct involved the use of violence, resulted in substantial financial gain or was conducted by a large number of persons in pursuit of a common purpose*” (CEDH, 2021, para. 369).

melhor opção (a via *necessária*) para proteger a segurança nacional, em uma sociedade democrática (CEDH, 2021, para. 338). Contudo, igualmente apontou que, para que determinado ato atentatório à proteção de dados seja considerado necessário, dever-se-ia igualmente observar a situação concreta do país, não podendo ser realizada uma análise abstrata (CEDH, 2021, para. 191 – p. 62; COUNCIL OF EUROPE, 1981).

Logo, relevante foi o comentário feito sobre o caso *Privacy International vs. Secretary of State for Foreign and Commonwealth Affairs and Others*, julgado pelo Tribunal de Justiça da União Europeia – TJUE – em 2020, visto que, neste julgado, ponderou-se que obrigar genericamente “*electronic communication services to disclose traffic data and location data to the security and intelligence agencies [...] exceeded the limits of what was strictly necessary*” para proteger a segurança nacional (CEDH, 2021, para. 238; tjue, 2020).

Já no que tange a proporcionalidade, esta se refere ao que se busca com a conduta almejada, isto é, o benefício esperado com a sua adoção, no caso, com a coleta, análise, armazenamento e transferência de dados, sendo imperiosa a existência de um “*legitimate prevailing interest*” em prol do Poder Público para que a proteção de dados possa ser violada (CEDH, 2021, para. 194 – p. 62-63; COUNCIL OF EUROPE, 2001, art. 2). No ponto, expressou-se ser importante balancear a seriedade da intrusão na esfera particular dos indivíduos e a importância da medida para que ela não seja considerada excessiva ou arbitrária (CEDH, 2021, para. 96 – p. 24).

Interessante notar que nem o fato de uma informação em potencial estar atrelada à segurança nacional seria suficiente para que a proteção de dados fosse levantada à luz da proporcionalidade. Sobre o tema, importante o destaque dado ao caso *Digital Rights Ireland Ltd. vs. Minister for Communications, Marine and Natural Resources and Others, and Kärntner Landesregierung and Others*, julgado pelo TJUE em 2014, visto que, neste, não se compreendeu como proporcional a violação da proteção de dados dos requerentes na medida em que não existiam provas capazes de sugerir que a sua conduta estivesse atrelada a um ilícito grave ou mesmo a um ato de terrorismo (CEDH, 2021, para. 210-211; TJUE, 2014). Mais do que isso, avultou-se ser necessário considerar a existência ou não de outros meios menos intrusivos para a obtenção da mesma informação, de modo que, se presentes, a proteção de dados não poderia ser violada, pois tida como desproporcional (CEDH, 2021, para. 96 – p. 26).

Ademais, se o material coletado se referir direta ou indiretamente à informação confidencial jornalística, especial consideração deveria ser dada para a sua realização em termos de proporcionalidade e necessidade, havendo um dever destes critérios estarem claramente documentados (CEDH, 2021, para. 96 – p. 26). Isso porque, uma eventual violação à proteção de dados destes profissionais “*could be a powerful disincentive to whistle-blowers*” (CEDH, 2021, para. 200), afetando significativamente o papel que a mídia, enquanto “Quarto Poder”, detém na fiscalização do Estado em matérias de interesse público (CEDH, 2021, para. 442).

Ainda, com o fito de evitar quaisquer abusos, a Corte apontou a necessidade de haver mecanismos de supervisão. A autoridade supervisora, assim sendo, deveria ter poderes para investigar e intervir junto àqueles que manuseiam/manusearão os dados, “*as well as the power to engage in legal proceedings or bring to the attention of competent judicial authorities violations of provisions of domestic law*” sobre o tema (CEDH, 2021, para. 194 – p. 62; COUNCIL OF EUROPE, 2001, art. 1). Nesse escopo, a CEDH determinou que seria “*desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure*” (CEDH, 2021, para. 336), até mesmo para que a citada margem de apreciação não seja, em si, abusiva, “*undermin[ing] or even destroy[ing] the proper functioning of democratic processes under the cloak of defending them*” (CEDH, 2021, para. 339).

Adicionalmente, deveria ter a possibilidade de ouvir reclamações de pessoas que eventualmente tenham tido seus direitos relativos à proteção de dados violados, sendo almejavél, ainda, a possibilidade de recorrer-se ao judiciário, em caso de negativa e/ou insatisfação por parte deste (CEDH, 2021, para. 194 – p. 63). Sobre o tema, relevante foi o debate sobre o caso *Maximillian Schrems vs. Data protection Commissioner*, julgado pelo TJUE em 2015, porquanto neste caso, que envolvia a transferência de dados do requerente do *Facebook* Irlanda para os Estados Unidos, discorreu-se sobre o direito fundamental de ter à disposição um remédio judicial efetivo para, inclusive, obter-se acesso, retificação ou apagamento de dados relativos à sua pessoa (CEDH, 2021, para. 226; TJUE, 2015).

Outrossim, para além de atuar *ex post facto*, mecanismos de supervisão também deveriam existir para agir *ex ante*, particularmente quando se tratando de autorizações para a interceptação, coleta, análise, retenção e compartilhamento de dados com terceiros Estados (CEDH, 2021, para. 197; COUNCIL OF EUROPE, 2015). Isso porque, nessa etapa, eventuais



violações poderiam ser evitadas, especialmente frente a jornalistas (CEDH, 2021, para. 232 e 440), se os critérios de necessidade e proporcionalidade fossem analisados por uma autoridade independente. No ponto, importante foi o destaque dado ao caso *Tele2 Sverige AB vs. Post-och telestyrelsen, and Secretary of State for the Home Department vs. Tom Watson and Others*, julgado pelo TJUE em 2016, pois, neste julgado, citou-se que a inexistência de “*precise rules providing for access to and use of retained data, and access to those data was not made dependent on prior review by a court or an independent administrative body*” seria ilegal (CEDH, 2021, para. 125; TJUE, 2016).

Com base nesses argumentos, por conseguinte, a CEDH criticou a falta de previsão legal específica por parte dos britânicos sobre a forma em que os dados eram analisados, recriminando notadamente o procedimento demasiadamente vago e aleatório adotado pelo Reino Unido para processar o *bulk data*. Teceu que a cybervigilância realizada, de cunho preventivo e indeterminado, demonstrava a falha legislativa britânica (pontualmente, o item número quatro dos elementos mínimos que uma legislação sobre interceptação de dados deveria prever), impactando diretamente no direito à vida privada (artigo 8) de todos os afetados (CEDH, 2021, para. 348-349 e 372).

Referente a isso, ainda, a Corte asseverou que, mesmo que os *warrants* e os *renewals* fossem feitos consoante a lei britânica (CEDH, 2021, para. 406), os analistas não necessitavam nem usar os termos contidos nos citados mandados (CEDH, 2021, para. 419). Desta forma, a falta de instrumentos de supervisão autônomos, segundo a CEDH, corroborara para a situação de violação, posto que, se existentes, eles poderiam averiguar a necessidade e proporcionalidade, autorizando e restringindo os parâmetros de busca utilizados pelos analistas para gerar as listas e, conseqüentemente, serem objeto de análise pormenorizada (CEDH, 2021, para. 350-352).

Veja-se que no *Regulation of Investigatory Powers Act* britânico, a supervisão ficaria a cargo do *Prime Minister of as Interceptions Comissunications Comissioner*, atrelado ao poder executivo, que tinha como objetivo revisar todos os atos dos analistas, até mesmo, obtendo acesso a documentos relevantes das atividades destes, sendo gerado um relatório anual depositado junto ao Parlamento Britânico, de acesso público (em que pese sujeito a detrações por questões de confidencialidade) (CEDH, 2021, para. 135-136). Não se tratava, portanto, de um órgão independente e imparcial que pudesse ser “*sufficiently robust to keep the*

*interference to what is necessary in a democratic society*” (CEDH, 2021, para. 356), culminando, assim, em uma violação do artigo 8.

Ademais, no que toca o compartilhamento das informações com a NSA, a Corte assentou que o Estado receptor também deveria possuir mecanismos de supervisão aptos a prevenir abusos e interferências desnecessárias e/ou desproporcionais, sendo essa uma das precauções que os britânicos deveriam adotar, consoante o item cinco dos requisitos mínimos legislativos sobre interceptação de dados (CEDH, 2021, para. 362).

Interessante referir que a CEDH expressou, porém, que em *todas* as etapas do procedimento adotado pela GCHQ, seja de aquisição e/ou interceptação, do apontamento de palavras-chave e do exame dos dados, além do seu potencial compartilhamento com as agências estrangeiras, deveriam estar sujeitos a uma análise de necessidade e proporcionalidade por órgão neutro e independente, mesmo que não fosse judicial (apesar de preferível), de modo que tal órgão (nacional ou estrangeiro) possa identificar se a medida era realmente necessária para os fins almejados, se outras formas menos intrusivas estariam disponíveis, ou mesmo quanto ao formato da coleta e processamento de dados (CEDH, 2021, para. 329-330, 372, 375, 377, 383, 387 e 395). Não sendo esse o caso, destarte, verificou-se não só a violação do artigo 8, senão também do artigo 10.

Afinal, considerando que as *“safeguards to be afforded to the press are of particular importance, and the protection of journalist sources is one of the cornerstones of freedom of the press”*, na ausência de uma autoridade imparcial certificadora preventiva, *“sources may be deterred from assisting the press in informing the public about matters of public interest”* por estarem potencialmente submetidas à coleta e ao processamento de seus dados (CEDH, 2021, para. 442 e 445). Isso, pois, as informações obtidas a partir da análise do *bulk data* poderiam acidentalmente cruzar-se com as comunicações (confidenciais) de jornalistas e suas fontes (CEDH, 2021, para. 448-450 e 453).

Ou seja, neste caso, a CEDH incorreu em debates de suma relevância no que tange a possibilidade de o Estado implementar a cybervigilância a partir da recepção, coleta, análise, arquivamento e transferência de dados, tecendo que, para além dos requisitos contidos nos próprios preceitos legais da Convenção Europeia de Direitos Humanos, outros parâmetros devem ser igualmente considerados, sobretudo, para se resguardar a legalidade da intrusão na esfera privada e na (eventual) limitação da liberdade de expressão no que toca o direito a ter acesso à informação de interesse coletivo.

Apesar de direcionada à conduta do Estado, tem-se que este caso também é de extrema importância para o setor privado, vez que o respeito para com os direitos humanos recai não apenas no Estado, senão também a todos aqueles situados dentro de sua jurisdição, pois vertical e horizontalmente oponíveis e exigíveis. Quer isso dizer que as gigantes de tecnologia também estariam obrigadas a proteger tais direitos<sup>194</sup>, tendo o dever de questionar eventuais abusos governamentais caso este eventualmente solicite acesso a dados, por exemplo.

Mais do que isso, justamente por não terem uma obrigação semelhante a do Estado de zelar pela ordem, segurança e interesse público, as empresas de tecnologia não poderiam direta ou indiretamente coletar, analisar ou mesmo reter dados sem o aval concreto do(s) interessado(s), sob pena de estarem igualmente incorrendo em um ato ilícito, ao qual, porém, cabe ao Estado onde tal coleta, análise ou retenção é feita, supervisionar e repreender. Entretanto, o que se vislumbra é um verdadeiro conluio entre esses sujeitos para a crescente vigilância do indivíduo na atual sociedade em rede.

Cabe, assim, às instâncias internacionais agirem em nome da tutela do indivíduo e de seus direitos intrínsecos, tal como se vislumbrou no caso aqui em comento, em que o Reino Unido fora condenado pela CEDH por violar o ‘direito ao respeito pela vida privada e familiar’ e a ‘liberdade de expressão’ no contexto de cybervigilância operada por meio da coleta, análise e retenção de dados.

#### 4 CONCLUSÃO

O mundo atual certamente introduz desafios à humanidade. O advento da sociedade em rede, trouxe mudanças significativas à sociedade, introduzindo um novo ambiente em que as pessoas podem se comunicar, inclusive, por outras formas e linguagens, as quais acabam gerando um número significativo de dados. Não por outra razão que as gigantes de tecnologia, dentro de um espaço altamente desregulado, tendo em suas mãos essas informações, utilizam-se das mesmas para o lançamento de novos produtos e serviços, muito embora, a um custo bastante alto, particularmente no que toca o respeito a certos direitos básicos do ser humano, como vida privada e a liberdade de escolha.

---

<sup>194</sup> “As empresas devem considerar os possíveis impactos de suas atividades sobre os direitos humanos, o que implicará, por exemplo, o monitoramento das atividades das filiais ou entidades que estão sob controle direto ou indireto da empresa mãe” (SALDANHA, 2018, p. 228).

O Estado, por outro lado, não resta inerte. Apesar deste ter o dever derivado do Contrato Social de regular a vida comum entre todos aqueles situados dentro de sua jurisdição, inclusive, no tocante à defesa dos direitos humanos, com o advento da sociedade informacional e da própria quantificação, o Estado tem igualmente utilizado-se dos dados produzidos pelos indivíduos nas redes e coletados pelas *big techs*, inaugurando um novo modelo de vigilância – a cibernética.

Ocorre que essa ‘sociedade do controle’, “viabilizad[a] pelo surgimento das novas tecnologias de informação, que garantem a possibilidade de regulação dos processos sociais sem que seja necessário detê-los dentro de espaços institucionais físicos”, como explicam Menezes Neto e Moraes (2018, p. 1133), não opera apenas para a garantia da prestação de serviços públicos ou mesmo para fins de segurança nacional e dos interesses coletivos. Os dados angariados, processados e armazenados também são usados contra os cidadãos para governar outros aspectos da vida humana, direcionando por vezes as próprias escolhas e opinião individual, sem contar a possibilidade de restringir o importante papel exercido pela mídia no controle dos atos públicos.

Como relatado no texto, o problema disso é que as movimentações instantâneas e constantes de dados realizadas a partir das redes não encontram balizas territoriais. Assim, o poder imponente que a informacionalidade crescente produz torna-se um problema para o Direito, haja vista o local em que este ocorre – nas próprias redes –, fora dos limites jurisdicionais dos Estados. Entretanto, por certo que a tecnologia da informação não é totalmente imaterial, pois dependem “de estruturas físicas que viabilizam a coleta e a transmissão de dados”, além dos locais em que a quantificação e a análise são realizadas (MENEZES NETO; MORAIS, 2018, p. 1136).

Nesse escopo é que o Direito corrente ainda pode ser de grande valia, tal como demonstrou-se a partir do caso *The Big Brother Watch et al.* apresentado neste texto. Isso porque, a CEDH, valendo-se de direitos positivados na Convenção Europeia de Direitos Humanos, entendeu pela responsabilização do Reino Unido pela realização da cybervigilância, conduzida pela coleta, análise, retenção e transferência de dados de pessoas situadas fora da região, asseverando que a sua conduta violava o direito à vida privada, constante no artigo 8, e a liberdade de expressão, prevista no artigo 10, do citado regramento.

Mais do que isso, este caso trouxe aspectos importantes que devem ser observados pelos Estados no que tange a eventuais limitações de tais direitos ocasionadas pela coleta e

processamento de *bulk data*, pois, para além da previsão específica em lei, a qual, inclusive, deve apresentar seis requisitos mínimos, elas devem ser consideradas necessárias e proporcionais – isso sem contar a necessidade de terem-se mecanismos de supervisão para que se possa averiguar a legalidade da conduta estatal – e, por que não, de todos aqueles que eventualmente manuseiam dados dentro deste – no contexto de cybervigilância.

Em vista disso, o caso comentado é sem dúvidas, paradigmático, denotando a justificativa de analisá-lo pormenorizadamente. Até mesmo porque, ao cabo, ele permite extrair uma mensagem bastante oportuna dentro deste novo contexto informacional gerado pela Sociedade em Rede, que é justamente a ideia de que as novas ferramentas podem ser usadas tanto para melhorarem a vida das pessoas em sociedade, como também podem trazer implicações importantes para o gozo de direitos já estabelecidos, de modo que a fixação de parâmetros extras suaviza a liquidificação constante da vida, como diria Bauman (2013, p. 3-7), e a própria intromissão pública e privada na intimidade do ser humano, sustentando, ainda, a existência de um ambiente social, em detrimento de um retorno a um eventual Estado de Natureza, que as redes parecem (re)introduzir.

## REFERÊNCIAS

AGÊNCIA CÂMARA. Congresso adia para a próxima semana sessão para análise de vetos. *Câmara Notícias*, 25 mai. 2022. Disponível em:

<https://www.camara.leg.br/noticias/878659-congresso-adia-para-a-proxima-semana-ssao-para-analise-de-vetos/>. Acesso em: 17 jun. 2022.

AGÊNCIA CÂMARA. Especialistas defendem responsabilidade compartilhada no combate às fake news. *Câmara de Notícias*, 19 ago. 2021. Disponível em:

<https://www.camara.leg.br/noticias/796855-especialistas-defendem-responsabilidade-compartilhada-no-combate-as-fake-news/>. Acesso em: 17 jun. 2022.

AGÊNCIA SENADO. Sancionada a revogação da Lei de Segurança Nacional; artigo contra disseminação de fake news é vetado. *Senado Notícias*, 02 set. 2021. Disponível em:

<https://www12.senado.leg.br/noticias/materias/2021/09/02/sancionada-a-revogacao-da-lei-de-seguranca-nacional-artigo-contradiseminacao-de-fake-news-e-vetado>. Acesso em: 17 jun. 2022.

BALL, J. NSA monitored calls of 35 world leaders after US official handed over contacts. *The Guardian*, 25 out. 2013. Disponível

em:<https://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls>. Acesso em: 12 jun. 2022.

BALKIN, J. The constitution in the national surveillance state. *Minnesota Law Review*, v. 93, n. 1, pp. 1-25, 2008.

BARCELOS, T. N. et al. Análise de fake news veiculadas durante a pandemia de COVID-19 no Brasil. *Revista Panamericana de Salud Publica*, n. 45, pp. 1-8, 2021. DOI: 10.26633/RPSP.2021.65.

BAUMAN, Z. *Vigilância Líquida: diálogos com David Lyon*. Trad. Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

BOLSONARO atacou a imprensa 87 vezes no 1º semestre de 2021, diz levantamento. *Poder 360*, 28 jul. 2021. Disponível em: <https://www.poder360.com.br/brasil/bolsonaro-atacou-imprensa-87-vezes-no-1o-semester-de-2021-diz-levantamento/>. Acesso em 17 jun. 2022.

BOVET, A., MAKSE, H.A. Influence of fake news in Twitter during the 2016 US presidential election. *Nature Communications*, v. 10, n. 7, 2019, DOI: 10.1038/s41467-018-07761-2.

CARDOSO, F. H. Prefácio. In: CASTELLS, M. *A Sociedade em rede*. 6ª ed. Trad. Roneide V. Majer. São Paulo: Paz e Terra, 1999.

CASTELLS, M. *A Sociedade em rede*. 6ª ed. Trad. Roneide V. Majer. São Paulo: Paz e Terra, 1999.

CEDH. Grand Chamber. *The Big Brother Watch et al. vs. Reino Unido*. Applications 58170/13, 62322/14 e 24960/15. Judgment of 25.05.2021. Disponível em: [https://hudoc.echr.coe.int/fre#{"itemid":\["001-210077"\]}](https://hudoc.echr.coe.int/fre#{). Acesso em: 10 jun. 2022.

CEDH. *Key cases 2021*: list of cases recommended by the Jurisconsult and approved by the Bureau. Estrasburgo, mar. 2021. Disponível em: [https://echr.coe.int/Documents/Cases\\_list\\_2021\\_ENG.pdf](https://echr.coe.int/Documents/Cases_list_2021_ENG.pdf). Acesso em: 09 jun. 2021.

CEDH. *Affaire Huvig v. France*. Application 11105/84. Judgment of 24.04 1990. Disponível em: [https://hudoc.echr.coe.int/fre#{"itemid":\["001-62184"\]}](https://hudoc.echr.coe.int/fre#{). Acesso em: 16 jun. 2022.

CEDH. *Affaire Valenzuela Contreras v. Spain*. Application 58/1997/842/1048. Judgment of 30.07.1998. Disponível em:

[https://hudoc.echr.coe.int/fre#%22itemid%22:\[%22001-62764%22\]](https://hudoc.echr.coe.int/fre#%22itemid%22:[%22001-62764%22]). Acesso em: 16 jun. 2022.

CEDH. *Gabriele Weber and Cesar Richard Saravia v. Germany*. Application 54934/00. Judgment of 29.06.2006. Disponível em:

[https://hudoc.echr.coe.int/fre#%22itemid%22:\[%22001-76586%22\]](https://hudoc.echr.coe.int/fre#%22itemid%22:[%22001-76586%22]). Acesso em: 16 jun. 2022.

CEDH. *Roman Zakharov v. Russia*. Application 47143/06. Judgment of 04.12.2015.

Disponível em: [https://hudoc.echr.coe.int/fre#%22itemid%22:\[%22002-10793%22\]](https://hudoc.echr.coe.int/fre#%22itemid%22:[%22002-10793%22]).

Acesso em: 16 jun. 2022.

CEDH. *Case of Kruslin v. France*, Application 11801/85. Judgment of 24.04.1990.

Disponível em:

<http://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-57626&filename=001-57626.pdf>. Acesso em: 16 jun. 2022.

CEDH. *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*. Application 58/1997/842/1048. Judgment of 28.06.2007. Disponível em:

[https://hudoc.echr.coe.int/fre#%22itemid%22:\[%22001-81323%22\]](https://hudoc.echr.coe.int/fre#%22itemid%22:[%22001-81323%22]). Acesso em: 16 jun. 2022.

COUNCIL OF EUROPE. *Convenção Europeia de Direitos Humanos*. Roma, 04 nov. 1950.

Disponível em: [https://www.echr.coe.int/documents/convention\\_por.pdf](https://www.echr.coe.int/documents/convention_por.pdf). Acesso em: 14 jun. 2022.

COUNCIL OF EUROPE. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. Strasbourg, 28 jan. 1981. Disponível em:

<https://rm.coe.int/1680078b37>. Acesso em: 15 jun. 2022.

COUNCIL OF EUROPE. *Explanatory report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. Strasbourg, 28 jan. 1981.

Disponível em: <https://rm.coe.int/16800ca434>. Acesso em: 15 jun. 2022.

COUNCIL OF EUROPE. *The Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory and transborder data flows*. Strasbourg, 08 nov. 2001. Disponível em:

<https://rm.coe.int/1680080626>. Acesso em: 15 jun. 2022.

COUNCIL OF EUROPE. *Report for Democracy through Law (“The Venice Commission”) on the Democratic Oversight of Signals Intelligence Agencies*. Strasbourg, 15.04.2015.

Disponível em:

[https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2015\)010-e](https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)010-e).

Acesso em: 14 jun. 2022.

GIUSSANI, A. Media and surveillance, the Predator scandal shakes Greece. *Osservatorio Balcani e Caucaso*, 19 mai. 2022. Disponível em:

<https://www.balcanicaucaso.org/eng/Areas/Greece/Media-and-surveillance-the-Predator-scandal-shakes-Greece-218223>. Acesso em: 13 jun. 2022

LEVITSKY, Steven; ZIBLATT, Daniel. *Como as democracias morrem*. Trad. Renato Aguiar. Rio de Janeiro: Zahar, 2018

LEVY, Pierre. *Cibercultura*. São Paulo: Ed. 34, 1999.

LINTHICUM, K. As El Salvador's president tries to silence free press, journalist brothers expose his ties to street gangs. *The San Diego Union Tribune*, 11 jun. 2022. Disponível em:

<https://www.sandiegouniontribune.com/latino-life/story/2022-06-11/nayib-bukele-el-salvador-el-faro-journalists>. Acesso em: 13 jun. 2022.

LÔBO, E; MORAIS, J. L. B. New technologies and the current communications model in the 2018 brazilian elections. *Novos Estudos Jurídicos*, v. 24, n. 3, pp. 1056-1087, set-dez 2019. DOI: 10.14210/nej.v24n3.p1056-1087

LOBO, E.; MORAIS, J. L. B.; NEMER, D. Democracia algorítmica: o futuro da democracia e o combate às milícias digitais no Brasil. *Revista Culturas Jurídicas*, v. 7, n. 17, pp. 255-276, mai./ago., 2020. DOI: 10.22409/rcj.v7i17.982

MARTINS, M. G.; TATEOKI, V. A. Proteção de dados pessoais e democracia: fake news, manipulação do eleitor e o caso da Cambridge Analytica. *REDES*, v. 7, n. 3, pp. 135-148, out. 2019. DOI: 10.18316/REDES.v7i3.5610).

MACASKILL, E.; BORGER, J.; GREENWALD, G. The National Security Agency: surveillance giant with eyes on America. *The Guardian*, 6 jun. 2013. Disponível em: <https://www.theguardian.com/world/2013/jun/06/national-security-agency-surveillance>. Acesso em 13 jun. 2022.

MARANHÃO, J.; ABRUSIO, J.; CAMPOS, R. Atribuição de responsabilidade das plataformas no combate às fake news. *Consultor Jurídico*, 16 jun. 2020. Disponível em: <https://www.conjur.com.br/2020-jun-16/direito-digital-responsabilidade-plataformas-combate-fake-news>. Acesso em 17 jun. 2022.



MASSIVE data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally. *Amnesty International*, 19 jul. 2021. Disponível em: <https://www.amnesty.org/en/latest/news/2021/07/the-pegasus-project/>. Acesso em: 13 jun. 2022.

MENEZES, R. F. "Admirável Mundo Novo": capitalismo de vigilância e risco à democracia. In: MORAIS, J. L. B. *Conexões: estado, direito e tecnologia*. Vitória: FDV Publicações, 2020.

MENEZES NETO, E. J.; MORAIS, J. L. B. Análises computacionais preditivas como um novo biopoder: modificações do tempo na sociedade dos sensores. *Novos Estudos Jurídicos*, v. 24, n. 3, pp. 1129-1154, set./dez 2018. DOI: 10.14210/nej.v24n3.p1129-1154

ORWELL, G. *1984*. São Paulo: Companhia das Letras, 2009.

OST, F. *O Tempo do Direito*. Trad. Maria Fernanda Oliveira. Lisboa: Instituto Piaget, 1999.

PARISER, E. *The filter bubble: How the new personalized web is changing what we read and how we think*. London: Penguin, 2011.

PEREIRA, M. R. desinformação como estratégia política: uma análise dos tweets de ataque à imprensa postados por Jair Messias Bolsonaro no ano de 2019. *Revista Aquila*, a. 12, n. 24, pp. 97-109, jan./jun. 2021. DOI: 10.17648/revista-aquila.v1i24.149.

PETERS, A. Privacy, Rechtsstaatlichkeit, and the Legal Limits on Extraterritorial Surveillance. In: MILLER, R. (Ed.) *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair*. Cambridge: Cambridge University press, 2017.

RIEMENSCHNEIDER P. S.; MUCELIN, G. A. B. Internet das Coisas, Decisões Automatizadas e o Direito à Explicação. *Rev. Fac. Dir. Uberlândia*, v. 49, n. 1, pp. 689-708, 2021. DOI: 10.14393/RFADIR-v49n1a2021-56135.

SALDANHA, J. Do direito soft ao direito hard em matéria de responsabilidade jurídica das empresas transnacionais por violação de direitos humanos. In: MORAIS, J. L. B. (Org). *Estado & Constituição: o fim do estado de direito*. Florianópolis: Tirant Lo Blanch, 2018.

SCHOSSLER, A. Economia faz Brasil deixar escândalo da NSA de lado. *Deutsche Welle*, 29 jun. 2015. Disponível em: <https://www.dw.com/pt-br/economia-faz-brasil-deixar-escandalo-da-nsa-de-lado/a-18550365>. Acesso em 13 jun. 2022.

SHULZE, M. Patterns of Surveillance Legitimization: The German Discourse on the NSA Scandal. *Surveillance & Society*, v. 13, n. 2, pp. 197-217, 2015. DOI: 10.24908/ss.v13i2.5296

SQUEFF, T. C.; MUCELIN, G. A. B. Contratos internacionais online de consumo: transformação digital desde o Mercosul. *RECHTD*, v. 13, n. 3, pp. 444-466, 2021. DOI: 10.4013/rechtd.2021.133.11.

SRNICEK, N. *Platform capitalism*. Cambridge: Polity Press, 2017.

TJUE. *Tele2 Sverige AB vs. Post-och telestyrelsen, and Secretary of State for the Home Department vs. Tom Watson and Others*. Cases C-203/15 and C-698/15. Judgment of 21.12.2016. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62015CJ0203>. Acesso em: 15 jun. 2022.

TJUE. *Digital Rights Ireland Ltd. vs. Minister for Communications, marine and Natural Resources and Others and Kärntner Landesregierung and Others*. Cases C-293/12 and c-594/12. Judgment of 8.04.2014. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293>. Acesso em: 15 jun. 2022.

TJUE. *Privacy International vs. Secretary of State for Foreign and Commonwealth Affairs and Others*. Case C-623/1. Judgment of 6.10.2020 Disponível em: <https://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-623/17> Acesso em: 15 jun. 2022.

TJUE. *Maximillian Schrems vs. Data protection Commissioner*. Case C-362/14. Judgment of 6.10.2015. Disponível em: <https://curia.europa.eu/juris/liste.jsf?num=C-362/14> . Acesso em: 15 jun. 2022.

THE world's most valuable resource is no longer oil, but data. *The Economist*, 6 mai. 2017. Disponível em: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. em: 12 jun. 2022.

UNITED NATIONS, *General Assembly Res. 69/166: The Right to Privacy in the Digital Age*. New York, 18 Dec. 2014, preâmbulo. Disponível em: <https://digitallibrary.un.org/record/788140>. Acesso em 17 jun. 2022.

WALKER, S. Viktor Orbán using NSO spyware in assault on media, data suggests. *The Guardian*, 18 jul. 2021. Disponível em:  
<https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests>. Acesso em: 13 jun. 2022

WIKILEAKS: EUA espionam Dilma e ministros brasileiros. *Deutsche Welle*, 4 jul. 2015. Disponível em:  
<https://www.dw.com/pt-br/wikileaks-eua-espionaram-dilma-e-ministros-brasileiros/a-18561907>. Acesso em: 13 jun. 2022






## BIOGRAFIA

### Tatiana Cardoso Squeff




Professora adjunta de Direito Internacional, Consumidor e Ambiental na UFRGS, e docente dos Programas de Pós-graduação em Direito da UFU e em Relações Internacionais da UFSM. Doutora em Direito Internacional pela UFRGS e Mestre em Direito pela UNISINOS. Pós-doutoranda em Direitos e Garantias Fundamentais na FDV. Especialista em Língua Inglesa, Direito Internacional, Relações Internacionais Contemporâneas e Direitos Humanos. Expert brasileira nomeada para atuar na Conferência da Haia em projetos de Direito Internacional Privado. Membro da ASADIP.

#### CONTATOS

 <http://lattes.cnpq.br/9206961411279490>  
 <https://orcid.org/0000-0001-9912-9047>  
 [tatiafrcardoso@gmail.com](mailto:tatiafrcardoso@gmail.com)

### Jose Luis Bolzan de Moraes

#### CONTATOS

 <http://lattes.cnpq.br/4650999047027866>  
 <https://orcid.org/0000-0002-0959-0954>  
 [bolzan@hotmail.com](mailto:bolzan@hotmail.com)

Graduado em Direito pela Universidade Federal de Santa Maria (1984), possui mestrado em Ciências Jurídicas pela Pontifícia Universidade Católica do Rio de Janeiro (1989) e doutorado em Direito pela Universidade Federal de Santa Catarina (1995). Docente do Programa de Pós-Graduação em Direito da Faculdade de Direito de Vitória (FDV) e da ATITUS. É procurador aposentado do Estado do Rio Grande do Sul e advogado.